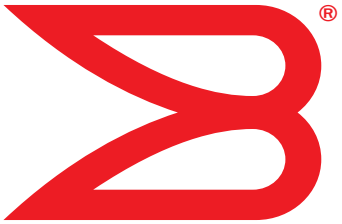
53-1003098-01
20 January 2014



Brocade Mobility RFS Controller

CLI Reference Guide

Supporting software release 5.5.0.0 and later

BROCADE

Brocade Communications Systems, Incorporated

Corporate and Latin American Headquarters
Brocade Communications Systems, Inc.
130 Holger Way
San Jose, CA 95134
Tel: 1-408-333-8000
Fax: 1-408-333-8101
E-mail: info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems China HK, Ltd.
No. 1 Guanghua Road
Chao Yang District
Units 2718 and 2818
Beijing 100020, China
Tel: +8610 6588 8888
Fax: +8610 6588 9999
E-mail: china-info@brocade.com

European Headquarters
Brocade Communications Switzerland Sàrl
Centre Swissair
Tour B - 4ème étage
29, Route de l'Aéroport
Case Postale 105
CH-1215 Genève 15
Switzerland
Tel: +41 22 799 5640
Fax: +41 22 799 5641
E-mail: emea-info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems Co., Ltd. (Shenzhen WFOE)
Citic Plaza
No. 233 Tian He Road North
Unit 1308 – 13th Floor
Guangzhou, China
Tel: +8620 3891 2000
Fax: +8620 3891 2111
E-mail: china-info@brocade.com

Document History

Title	Publication number	Summary of changes	Date
Brocade Mobility RFS Controller CLI Reference Guide	53-1003098-01	New Additions for software version 5.5.0.0	January 2014

Contents

About This Guide

In this chapter

Supported hardware and software

This guide provides information on using the following Brocade wireless controllers and access points:

- Brocade Mobility RFS7000 Controller
- Brocade Mobility RFS6000 Controller
- Brocade Mobility RFS4000 Controller
- Brocade Mobility RFS9510 Controller
- Brocade Mobility 71XX Series Access Point
- Brocade Mobility 650 Access Point
- Brocade Mobility 6511 Access Point
- Brocade Mobility 1220 Access Point
- Brocade Mobility 1240 Access Point

Document Conventions

This section describes text formatting conventions and important notice formats used in this document.

Text formatting

The narrative-text formatting conventions that are used are as follows:

bold text	Identifies command names
	Identifies the names of user-manipulated GUI elements
	Identifies keywords
	Identifies text to enter at the GUI or CLI
italic text	Provides emphasis
	Identifies variables
	Identifies document titles
`code` text	Identifies CLI output

For readability, command names in the narrative portions of this guide are presented in bold; for example, **show version**.

Notes

The following notice statement is used in this manual.

NOTE
A note provides a tip, guidance or advice, emphasizes important information, or provides a reference to related information.

Understanding command syntax

<variable>	Variables are described with a short description enclosed within a '<' and a '>' pair.
	For example, the command,
	`RFController>show interface ge 1`
	is documented as
	`show interface ge <idx>`
	• show – The command – Display information
	• interface – The keyword – The interface
	• <idx> – The variable – ge Index value

|	The pipe symbol. This is used to separate the variables/keywords in a list.
	For example, the command
	`RFController> show .....`
	is documented as
	`show [adoption|advanced-wips|boot|captive-portal|......]`
	where:
	• show – The command
	• [adoption|advanced-wips|boot|captive-portal|.....] – Indicates the different commands that can be combined with the show command. However, only one of the above list can be used at a time.
	`show adoption ...`
	`show advanced-wips ...`
	`show boot ...`

[]	Of the different keywords and variables listed inside a '[' & ']' pair, only one can be used. Each choice in the list is separated with a '|' (pipe) symbol.
	For example, the command
	`RFController# clear ...`
	is documented as
	`clear [arp-cache|cdp|crypto|event-history| firewall|ip|spanning-tree]`
	where:
	• clear – The command
	• [arp-cache|cdp|crypto|event-history|firewall|ip|spanning-tree] – Indicates that seven keywords are available for this command and only one can be used at a time

{ }	Any command/keyword/variable or a combination of them inside a '{' & '}' pair is optional. All optional commands follow the same conventions as listed above. However they are displayed italicized.
	For example, the command
	`RFController> show adoption ....`
	is documented as
	`show adoption info` *`{on <DEVICE-OR-DOMAIN-NAME>}`*
	Here:
	• show adoption info – The command. This command can also be used as
	`show adoption info`
	• {on <DEVICE-OR-DOMAIN-NAME>} – The optional keyword *on* <*device-or-domain-name*>. The command can also be extended as
	`show adoption info` *`{on <DEVICE-OR-DOMAIN-NAME>}`*
	Here the keyword *{on <DEVICE-OR-DOMAIN-NAME>}* is optional.

command / keyword	The first word is always a command. Keywords are words that must be entered as is. Commands and keywords are mandatory.
	For example, the command,
	`RFController>show wireless`
	is documented as
	`show wireless`
	where:
	• show – The command
	• wireless – The keyword

Related publications

The following Brocade Communications Systems, Inc. documents supplement the information in this guide and can be located at http://www.brocade.com/ethernetproducts.

- *Brocade Mobility RFS Controller System Reference Guide* - Describes configuration of the Brocade wireless controllers using the Web UI.
- *Brocade Mobility RFS Controller CLI Reference Guide* (this document) - Describes the *Command Line Interface* (CLI) and *Management Information Base* (MIB) commands used to configure the Brocade wireless controllers.

If you find errors in the guide, send an e-mail to documentation@brocade.com.

Getting technical help

To contact Technical Support, go to http://www.brocade.com/services-support/index.page for the latest e-mail and telephone contact information.

Chapter

INTRODUCTION 1

This chapter describes the commands available within a device's *Command Line Interface* (CLI) structure. CLI is available for wireless controllers, *access points* (APs), and service platforms.

Access the CLI by using:

- A terminal emulation program running on a computer connected to the serial port on the device (access point, wireless controller, and service platform).
- A Telnet session through *Secure Shell* (SSH) over a network.

Configuration for connecting to a Controller using a terminal emulator

If connecting through the serial port, use the following settings to configure your terminal emulator:

Bits Per Second	19200
Data Bits	8
Parity	None
Stop Bit	1
Flow Control	None

When a CLI session is established, complete the following (user input is in **bold**):

```
login as: <username>
administrator's login password: <password>
```

User Credentials

Use the following credentials when logging into a device for the first time:

User Name	admin
Password	admin123

When logging into the CLI for the first time, you are prompted to change the password.

Examples in this reference guide

Examples used in this reference guide are generic to each supported wireless controller, service platform, and AP model. Commands that are not common, are identified using the notation "Supported in the following platforms." For an example, see below:

Supported in the following platforms:

- Wireless Controller – Brocade Mobility RFS6000

The above example indicates the command is only available for a Brocade Mobility RFS6000 model wireless controller.

1

CLI Overview

The CLI is used for configuring, monitoring, and maintaining the network. The user interface allows you to execute commands on supported wireless controllers, service platforms, and APs, using either a serial console or a remote access method.

This chapter describes basic CLI features. Topics covered include an introduction to command modes, navigation and editing features, help features and command history.

The CLI is segregated into different command modes. Each mode has its own set of commands for configuration, maintenance, and monitoring. The commands available at any given time depend on the mode you are in, and to a lesser extent, the particular model used. Enter a question mark (?) at the system prompt to view a list of commands available for each command mode/instance.

Use specific commands to navigate from one command mode to another. The standard order is: USER EXEC mode, PRIV EXEC mode and GLOBAL CONFIG mode.

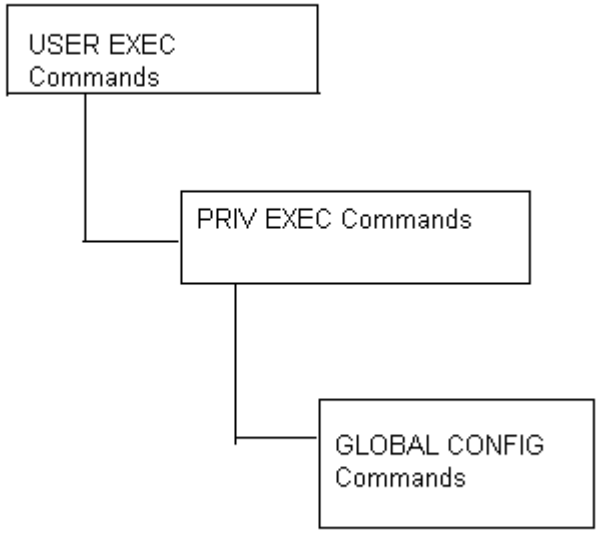


FIGURE 1 Hierarchy of User Modes

Command Modes

A session generally begins in the USER EXEC mode (one of the two access levels of the EXEC mode). For security, only a limited subset of EXEC commands are available in the USER EXEC mode. This level is reserved for tasks that do not change the device's (wireless controller, service platform, or AP) configuration.

```
rfs7000-37FABE>
```

The system prompt signifies the device name and the last three bytes of the device MAC address.

To access commands, enter the PRIV EXEC mode (the second access level for the EXEC mode). Once in the PRIV EXEC mode, enter any EXEC command. The PRIV EXEC mode is a superset of the USER EXEC mode.

```
rfs7000-37FABE>enable
rfs7000-37FABE#
```

Most of the USER EXEC mode commands are one-time commands and are not saved across device reboots. Save the command by executing ‘commit’ command. For example, the show command displays the current configuration and the clear command clears the interface.

Access the GLOBAL CONFIG mode from the PRIV EXEC mode. In the GLOBAL CONFIG mode, enter commands that set general system characteristics. Configuration modes, allow you to change the running configuration. If you save the configuration later, these commands are stored across device reboots.

Access a variety of protocol specific (or feature-specific) modes from the global configuration mode. The CLI hierarchy requires you to access specific configuration modes only through the global configuration mode.

```
rfs7000-37FABE# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
rfs7000-37FABE(config)#
```

You can also access sub-modes from the global configuration mode. Configuration sub-modes define specific features within the context of a configuration mode.

```
rfs7000-37FABE(config)# aaa-policy test
rfs7000-37FABE(config-aaa-policy-test)#
```

Table 1 summarizes available CLI commands.

TABLE 1 Controller CLI Modes and Commands

User Exec Mode	Priv Exec Mode	Global Configuration Mode
captive-portal-page-upload	archive	aaa-policy
change-passwd	boot	aaa-tacacs-policy
clear	captive-portal-page-upload	advanced-wips-policy
clock	cd	alias
create-cluster	cluster	br650
crypto	commit	br6511
device-upgrade	connect	br1220
help	crypto	br71xx
join-cluster	debug	br81xx
logging	device-upgrade	association-acl-policy
mint	diff	auto-provisioning-policy
no	dir	captive-portal
page	disable	clear
ping	edit	client-identity
revert	enable	client-identity-group
service	erase	clone
show	halt	customize
ssh	help	device
telnet	join-cluster	device-categorization

TABLE 1 Controller CLI Modes and Commands

User Exec Mode	Priv Exec Mode	Global Configuration Mode
terminal	l2tpv3	dhcp-server-policy
time-it	logging	dns-whitelist
traceroute	mint	event-system-policy
watch	mkdir	firewall-policy
write	more	global-association-list
clrscr	no	help
exit	page	host
virtual-machine (Brocade Mobility RFS9510)	pwd	inline-password-encryption
	re-elect	ip
	reload	l2tpv3
	remote-debug	mac
	rename	management-policy
	revert	meshpoint
	rmdir	meshpoint-qos-policy
	self	mint-policy
	service	nac-list
	show	no
	ssh	passpoint-policy
	telnet	password-encryption
	terminal	profile
	time-it	radio-qos-policy
	traceroute	radius-group
	upgrade	radius-server-policy
	upgrade-abort	radius-user-pool-policy
	watch	rename
	clrscr	rf-domain
	exit	rfs4000
	virtual-machine (Brocade Mobility RFS9510)	rfs7000
		role-policy
		routing-policy
		self
		smart-rf-policy
		wips-policy
		wlan
		wlan-qos-policy

TABLE 1 Controller CLI Modes and Commands

User Exec Mode	Priv Exec Mode	Global Configuration Mode
		write
		clrscr
		commit
		do
		end
		exit
		revert
		service
		show

Getting Context Sensitive Help

Enter a question mark (?) at the system prompt to display a list of commands available for each mode. Obtain a list of arguments and keywords for any command using the CLI context-sensitive help.

Use the following commands to obtain help specific to a command mode, command name, keyword or argument:

Command	Description
(prompt)# help	Displays a brief description of the help system
(prompt)# abbreviated-command-entry?	Lists commands in the current mode that begin with a particular character string
(prompt)# abbreviated-command-entry<Tab>	Completes a partial command name
(prompt)# ?	Lists all commands available in the command mode
(prompt)# command ?	Lists the available syntax options (arguments and keywords) for the command
(prompt)# command keyword ?	Lists the next available syntax option for the command

NOTE
The system prompt varies depending on the configuration mode.

NOTE
Enter Ctrl + V to use ? as a regular character and not as a character used for displaying context sensitive help. This is required when the user has to enter a URL that ends with a ?

NOTE
The escape character used through out the CLI is “\”. To enter a "\" use "\\" instead.

When using context-sensitive help, the space (or lack of a space) before the question mark (?) is significant. To obtain a list of commands that begin with a particular sequence, enter the characters followed by a question mark (?). Do not include a space. This form of help is called word help, because it completes a word.

```
rfs7000-37FABE#service?
service Service Commands
rfs7000-37FABE#service
```

Enter a question mark (?) (in place of a keyword or argument) to list keywords or arguments. Include a space before the “?”. This form of help is called command syntax help. It shows the keywords or arguments available based on the command/keyword and argument already entered.

```
rfs7000-37FABE#service ?
  advanced-wips                     Advanced WIPS service commands
 block-adopter-config-update       Block configuration updates from the
                                    adopter
  clear                             Clear adoption history
  cli-tables-skin                   Choose a formatting layout/skin for CLI
                                    tabular outputs
  cluster                           Cluster Protocol
  copy                              Copy from one file to another
  delete                            Delete sessions
  delete-offline-aps                Delete Access Points that are configured
                                    but offline
  force-send-config                 Resend configuration to the device
  force-update-vm-stats             Force VM statistics to be pushed up to the
                                    NOC
  load-balancing                    Wireless load-balancing service commands
  locator                           Enable leds flashing on the device
  mint                              MiNT protocol
  pktcap                            Start packet capture
  pm                                Process Monitor
  radio                             Radio parameters
  radius                            Radius test
  request-full-config-from-adopter  Request full configuration from the
                                    adopter
  set                               Set validation mode
  show                              Show running system information
  signal                            Send a signal to a process
  smart-rf                          Smart-RF Management Commands
  ssm                               Command related to ssm
  start-shell                       Provide shell access
  trace                             Trace a process for system calls and
                                    signals
  wireless                          Command related to wireless


rfs7000-37FABE#
```

It is possible to abbreviate commands and keywords to allow a unique abbreviation. For example, “configure terminal” can be abbreviated as `config t`. Since the abbreviated command is unique, the controller accepts the abbreviation and executes the command.

Enter the help command (available in any command mode) to provide the following description:

```
rfs7000-37FABE>help

When using the CLI, help is provided at the command line when typing '?'.
```

```
If no help is available, the help content will be empty. Backup until entering
a '?'
shows the help content.

There are two styles of help provided:
1. Full help. Available when entering a command argument (e.g. 'show ?'). This
will
   describe each possible argument.

2. Partial help. Available when an abbreviated argument is entered. This will
display
   which arguments match the input (e.g. 'show ve?').

rfs7000-37FABE>
```

Using the No Command

Almost every command has a no form. Use no to disable a feature or function or return it to its default. Use the command without the no keyword to re-enable a disabled feature.

Basic Conventions

Keep the following conventions in mind while working within the CLI structure:

- Use ? at the end of a command to display available sub-modes. Type the first few characters of the sub-mode and press the tab key to add the sub-mode. Continue using ? until you reach the last sub-mode.
- Pre-defined CLI commands and keywords are case-insensitive: cfg = Cfg = CFG. However (for clarity), CLI commands and keywords are displayed (in this guide) using mixed case. For example, apPolicy, trapHosts, channelInfo.
- Enter commands in uppercase, lowercase, or mixed case. Only passwords are case sensitive.

Using CLI Editing Features and Shortcuts

A variety of shortcuts and edit features are available. The following sections describe these features:

- *Moving the Cursor on the Command Line*
- *Completing a Partial Command Name*
- *Command Output pagination*

Moving the Cursor on the Command Line

Table 2 shows the key combinations or sequences to move the command line cursor. Ctrl defines the control key, which must be pressed simultaneously with its associated letter key. Esc means the escape key (which must be pressed first), followed by its associated letter key. Keys are not case sensitive. Specific letters are used to provide an easy way of remembering their functions. In Table 2, bold characters indicate the relation between a letter and its function.

TABLE 2 Keystrokes Details

Keystrokes	Function Summary	Function Details
Left Arrow or Ctrl-B	Back character	Moves the cursor one character to the left When entering a command that extends beyond a single line, press the Left Arrow or Ctrl-B keys repeatedly to move back to the system prompt.
Right Arrow or Ctrl-F	Forward character	Moves the cursor one character to the right
Esc- B	Back word	Moves the cursor back one word
Esc- F	Forward word	Moves the cursor forward one word
Ctrl-A	Beginning of line	Moves the cursor to the beginning of the command line
Ctrl-E	End of line	Moves the cursor to the end of the command line
Ctrl-D		Deletes the current character
Ctrl-U		Deletes text up to cursor
Ctrl-K		Deletes from the cursor to end of the line
Ctrl-P		Obtains the prior command from memory
Ctrl-N		Obtains the next command from memory
Esc-C		Converts the letter at the cursor to uppercase
Esc-L		Converts the letter at the cursor to lowercase
Esc-D		Deletes the remainder of a word
Ctrl-W		Deletes the word up to the cursor
Ctrl-Z		Returns to the root prompt
Ctrl-T		Transposes the character to the left of the cursor with the character located at the cursor
Ctrl-L		Clears the screen

Completing a Partial Command Name

If you cannot remember a command name (or if you want to reduce the amount of typing you have to perform), enter the first few letters of a command, then press the Tab key. The command line parser completes the command if the string entered is unique to the command mode. If your keyboard does not have a Tab key, press Ctrl-L.

The CLI recognizes a command once you have entered enough characters to make the command unique. If you enter “conf” within the privileged EXEC mode, the CLI associates the entry with the configure command, since only the configure command begins with `conf`.

In the following example, the CLI recognizes a unique string in the privileged EXEC mode when the Tab key is pressed:

```
rfs7000-37FABE# conf<Tab>
rfs7000-37FABE# configure
```

When using the command completion feature, the CLI displays the full command name. The command is not executed until the Return or Enter key is pressed. Modify the command if the full command was not what you intended in the abbreviation. If entering a set of characters (indicating more than one command), the system lists all commands beginning with that set of characters.

Enter a question mark (?) to obtain a list of commands beginning with that set of characters. Do not leave a space between the last letter and the question mark (?).

For example, entering U lists all commands available in the current command mode:

```
rfs7000-37FABE#co?
  commit     Commit all changes made in this session
  configure  Enter configuration mode
  connect    Open a console connection to a remote device
  copy       Copy from one file to another

rfs7000-37FABE#
```

NOTE
The characters entered before the question mark are reprinted to the screen to complete the command entry.

Command Output pagination

Output often extends beyond the visible screen length. For cases where output continues beyond the screen, the output is paused and a

```
--More--
```

prompt displays at the bottom of the screen. To resume the output, press the Enter key to scroll down one line or press the Spacebar to display the next full screen of output.

Creating Profiles

Profiles are sort of a ‘template’ representation of configuration. The system has:

- a default profile for each of the following devices:
  - Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- a default profile for each of the following service platforms:
  - Brocade Mobility RFS9510
- a default profile for each of the following access points:

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

To modify the default profile to assign an IP address to the management port:

```
rfs7000-37FABE(config)#profile rfs7000 default-rfs7000
rfs7000-37FABE(config-profile-default-rfs7000)#interface me1
rfs7000-37FABE(config-profile-default-rfs7000-if-me1)#ip address
172.16.10.2/24
rfs7000-37FABE(config-profile-default-rfs7000-if-me1)#commit
rfs7000-37FABE(config-profile-default-rfs7000)#exit
rfs7000-37FABE(config)#
```

The following command displays a default Brocade Mobility 71XX Access Point profile:

```
rfs7000-37FABE(config)#profile br71xx default-br71xx
rfs7000-37FABE(config-profile-default-br71xx)#
rfs7000-37FABE(config-profile-default-br71xx)#show context
profile br71xx default-br71xx
 autoinstall configuration
 autoinstall firmware
 device-upgrade persist-images
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 crypto remote-vpn-client
 interface radio1
 interface radio2
 interface radio3
 interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge2
  ip dhcp trust
  qos trust dscp
--More--
```

Change the default profile by creating vlan 150 and mapping to ge3 Physical interface

Logon to the controller in config mode and follow the procedure below:

```
rfs7000-37FABE(config-profile-default-rfs7000)# interface vlan 150
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan150)# ip address
192.168.150.20/24
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan150)# exit
rfs7000-37FABE(config-profile-default-rfs7000)# interface ge 3
rfs7000-37FABE(config-profile-default-rfs7000-if-ge3)# switchport access vlan
150
rfs7000-37FABE(config-profile-default-rfs7000-if-ge3)# commit write
[OK]
rfs7000-37FABE(config-profile-default-rfs7000-if-ge3)# show interface vlan 150
Interface vlan150 is UP
  Hardware-type: vlan, Mode: Layer 3, Address: 00-15-70-37-FA-BE
  Index: 8, Metric: 1, MTU: 1500
  IP-Address: 192.168.150.20/24
    input packets 43, bytes 12828, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 0, bytes 0, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
```

Viewing Configured APs

To view previously configured APs, enter the following command:

```
rfs7000-37FABE(config)#show wireless br configured
--------------------------------------------------------------------------------
--------
 IDX      NAME             MAC            PROFILE      RF-DOMAIN    ADOPTED-BY
--------------------------------------------------------------------------------
--------
  1   br71xx-4AA708   00-04-96-4A-A7-08   default-br71xx   default
un-adopted
  2   br71xx-11E6C4   00-23-68-11-E6-C4   default-br71xx   default
un-adopted
  3   br650-000001    00-A0-F8-00-00-01   default-br650    default
un-adopted
--------------------------------------------------------------------------------
--------
rfs7000-37FABE(config)#
```

Remote Administration

A terminal server may function in remote administration mode if either the terminal services role is not installed on the machine or the client used to invoke the session has enabled the admin controller.

- A terminal emulation program running on a computer connected to the serial port on the controller. The serial port is located on the front of the controller.
- A Telnet session through a *Secure Shell* (SSH) over a network. The Telnet session may or may not use SSH depending on how the controller is configured. Brocade recommends using SSH for remote administration tasks.

Configuring Telnet for Management Access

Login through the serial console. Perform the following:

1. A session generally begins in the USER EXEC mode (one of the two access levels of the EXEC mode).
2. Access the GLOBAL CONFIG mode from the PRIV EXEC mode.

   ```
   rfs7000-37FABE> en
   rfs7000-37FABE# configure terminal
   Enter configuration commands, one per line.  End with CNTL/Z.
   ```

3. Go to ‘default-management-policy’ mode.

   ```
   rfs7000-37FABE(config)# management-policy ?
   rfs7000-37FABE(config)# management-policy default
   rfs7000-37FABE(config-management-policy-default)#
   ```

4. Enter Telnet and the port number at the command prompt. The port number is optional. The default port is 23. Commit the changes after every command. Telnet is enabled.

   ```
   rfs7000-37FABE(config-management-policy-default)# telnet
   rfs7000-37FABE(config-management-policy-default)# commit write
   ```

5. Connect to the controller through Telnet using its configured IP address. Use the following credentials when logging on to the device for the first time:

User Name	admin
Password	admin123

When logging into the controller for the first time, you are prompted to change the password.

To change user credentials:

1. Enter the username, password, role and access details.

```
rfs7000-37FABE(config-management-policy-default)#user testuser password
admin123
 role helpdesk access all
rfs7000-37FABE(config-management-policy-default)# commit
rfs7000-37FABE(config-management-policy-default)#show context
management-policy default
 telnet
 http server
 https server
 ssh
 user admin password 1
ba7da2bf2f7945af1d3ae1b8b762b541bd5bac1f80a54cd4488f38ed44b91ecd role
superuser access all
 user operator password 1
0be97e9e30d29dfc4733e7c5f74a7be54570c2450e855cea1a696b0558a40401 role monitor
access all
 user testuser password 1
bca381b5b93cddb0c209e1da8a9d387fa09bfae14cc987438a4d144cb516ffcb role
helpdesk access all
 snmp-server community public ro
 snmp-server community private rw
 snmp-server user snmptrap v3 encrypted des auth md5 0
 snmp-server user snmpoperator v3 encrypted des auth md5 0 operator
 snmp-server user snmpmanager v3 encrypted des auth md5 0
rfs7000-37FABE(config-management-policy-default)#
```

2. Logon to the Telnet console and provide the user details configured in the previous step to access the controller.

```
rfs7000 release  5.5.0.0-018D
rfs7000-37FABE login: testuser
Password:
Welcome to CLI
Starting CLI...
rfs7000-37FABE>
```

Configuring SSH

By default, SSH is enabled from the factory settings on the controller. The controller requires an IP address and login credentials.

To enable SSH access in the default profile, login through the serial console. Perform the following:

1. Access the GLOBAL CONFIG mode from the PRIV EXEC mode.

```
rfs7000-37FABE> en
rfs7000-37FABE# configure
Enter configuration commands, one per line.  End with CNTL/Z.
```

2. Go to ‘default-management-policy’ mode.

```
rfs7000-37FABE(config)# management-policy default
rfs7000-37FABE(config-management-policy-default)#
```

3. Enter SSH at the command prompt.

```
rfs7000-37FABE(config-management-policy-default)# ssh
```

4. Log into the controller through SSH using appropriate credentials.
5. Use the following credentials when logging on to the device for the first time:

User Name	admin
Password	admin123

When logging into the controller for the first time, you are prompted to change the password.

To change the user credentials:

```
rfs7000 release 5.5.0.0-018D
rfs7000-37FABE login: testuser
Password:
Welcome to CLI
Starting CLI...
rfs7000-37FABE>
```

Chapter

USER EXEC MODE COMMANDS

2

Logging in to the wireless controller places you within the USER EXEC command mode. Typically, a login requires a user name and password. You have three login attempts before the connection attempt is refused. USER EXEC commands (available at the user level) are a subset of the commands available at the privileged level. In general, USER EXEC commands allow you to connect to remote devices, perform basic tests, and list system information.

To list available USER EXEC commands, use ? at the command prompt. The USER EXEC prompt consists of the device host name followed by an angle bracket (>).

```
<DEVICE>>?
Command commands:
  captive-portal-page-upload  Captive portal advanced page upload
  change-passwd               Change password
  clear                       Clear
  clock                       Configure software system clock
  cluster                     Cluster commands
  commit                      Commit all changes made in this session
  connect                     Open a console connection to a remote device
  create-cluster              Create a cluster
  crypto                      Encryption related commands
  debug                       Debugging functions
  device-upgrade              Device firmware upgrade
  disable                     Turn off privileged mode command
  enable                      Turn on privileged mode command
  help                        Description of the interactive help system
  join-cluster                Join the cluster
  l2tpv3                      L2tpv3 protocol
  logging                     Modify message logging facilities
  mint                        MiNT protocol
  no                          Negate a command or set its defaults
  page                        Toggle paging
  ping                        Send ICMP echo messages
  revert                      Revert changes
  service                     Service Commands
  show                        Show running system information
  smart-cache                 Content Cache Operation
  ssh                         Open an ssh connection
  telnet                      Open a telnet connection
  terminal                    Set terminal line parameters
  time-it                     Check how long a particular command took between
                              request and completion of response
  traceroute                  Trace route to destination
  virtual-machine             Virtual Machine
  watch                       Repeat the specific CLI command at a periodic
                              interval
  write                       Write running configuration to memory or
                              terminal

  clrscr                      Clears the display screen
  exit                        Exit from the CLI
```

2

<DEVICE>>

User Exec Commands

Table 1 summarizes the User Exec Mode commands.

TABLE 1 User Exec Mode Commands

Command	Description	Reference
captive-portal-page-upload	Uploads captive portal advanced pages	page 17
change-passwd	Changes the password of a logged user	page 19
clear	Resets the last saved command	page 19
clock	Configures the system clock	page 26
cluster	Accesses the cluster context	page 27
connect	Establishes a console connection to a remote device	page 28
create-cluster	Creates a new cluster on a specified device	page 29
crypto	Enables encryption	page 30
device-upgrade	Configures device firmware upgrade settings	page 39
disable	Turns off (disables) the privileged mode command set	page 49
enable	Turns on (enables) the privileged mode command set	page 50
join-cluster	Adds a device (access point, wireless controller, or service platform) to an existing cluster of devices	page 50
l2tpv3	Establishes or brings down *Layer 2 Tunneling Protocol Version 3* (L2TPV3) tunnels	page 51
logging	Modifies message logging facilities	page 53
mint	Configures MiNT protocol	page 54
no	Negates a command or sets its default	page 55
page	Toggles a device's (access point, wireless controller, or service platform) paging function	page 59
ping	Sends ICMP echo messages to a user-specified location	page 59
ssh	Opens an SSH connection between two network devices	page 60
telnet	Opens a Telnet session	page 61
terminal	Sets the length and width of the terminal window	page 62
time-it	Verifies the time taken by a particular command between request and response	page 62
traceroute	Traces the route to its defined destination	page 63
watch	Repeats a specific CLI command at a periodic interval	page 64
virtual-machine	Installs, configures, and monitors the status of *virtual machines* (VMs). This command is specific to the Brocade Mobility RFS9510 series service platforms.	page 65
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394

TABLE 1 User Exec Mode Commands (Continued)

Command	Description	Reference
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425
exit	Ends the current CLI session and closes the session window	page 65

captive-portal-page-upload

User Exec Commands

Uploads captive portal advanced pages

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
captive-portal-page-upload [<CAPTIVE-PORTAL-NAME>|cancel-upload|load-file]

captive-portal-page-upload <CAPTIVE-PORTAL-NAME>
[<MAC/HOSTNAME>|all|rf-domain]
captive-portal-page-upload <CAPTIVE-PORTAL-NAME> [<MAC/HOSTNAME>|all]
          {upload-time <TIME>}
captive-portal-page-upload <CAPTIVE-PORTAL-NAME> rf-domain
[<DOMAIN-NAME>|all]
          {from-controller} {(upload-time <TIME>)}

captive-portal-page-upload cancel-upload [<MAC/HOSTNAME>|all|on rf-domain
[<DOMAIN-
          NAME>|all]]
captive-portal-page-upload load-file <CAPTIVE-PORTAL-NAME> <URL>
```

Parameters

```
captive-portal-page-upload <CAPTIVE-PORTAL-NAME> [<MAC/HOSTNAME>|all]
{upload-time <TIME>}
```

captive-portal-page-upload <CAPTIVE-PORTAL-NAME>	Uploads advanced pages of the captive-portal identified by the <CAPTIVE-PORTAL-NAME> parameter • <CAPTIVE-PORTAL-NAME> – Specify the captive portal's name (should be existing and configured).
<MAC/HOSTNAME>	Uploads to a specified AP • <MAC/HOSTNAME> – Specify AP's MAC address or hostname.
all	Uploads to all APs
upload-time <TIME>	Optional. Configures an AP upload time • <TIME> – Specify upload time in the MM/DD/YYYY-HH:MM or HH:MM format.

	`captive-portal-page-upload <CAPTIVE-PORTAL-NAME> rf-domain [<DOMAIN-NAME>|all]` *`{from-controller} {(upload-time <TIME>)}`*
captive-portal-page-upload <CAPTIVE-PORTAL-NAME>	Uploads advanced pages of the captive portal identified by the <CAPTIVE-PORTAL-NAME> parameter • <CAPTIVE-PORTAL-NAME> – Specify captive portal's name (should be existing and configured).
rf-domain [<DOMAIN-NAME>|all]	Uploads to all APs within a specified RF Domain or all RF Domains • <DOMAIN-NAME> – Uploads to APs within a specified RF Domain. Specify the RF Domain name. • all – Uploads to APs across all RF Domains
from-controller	Optional. Uploads to APs from the adopted device
upload-time <TIME>	Optional. Configures an AP upload time • <TIME> – Specify upload time in the MM/DD/YYYY-HH:MM or HH:MM format.
	`captive-portal-page-upload cancel-upload [<MAC/HOSTNAME>|all|on rf-domain [<DOMAIN-NAME>|all]]`
captive-portal-page-upload cancel-upload	Cancels a scheduled AP upload
cancel-upload [<MAC/HOSTNAME>| all|on rf-domain [<DOMAIN-NAME>| all]	Select one of the following options: • <MAC/HOSTNAME> – Cancels scheduled upload to a specified AP. Specify the AP's MAC address or hostname • all – Cancels all scheduled AP uploads • on rf- domain – Cancels all scheduled uploads within a specified RF Domain or all RF Domains • <DOMAIN-NAME> – Cancels scheduled uploads within a specified RF Domain. Specify RF Domain name. • all – Cancels scheduled uploads across all RF Domains
	`captive-portal-page-upload load-file <CAPTIVE-PORTAL-NAME> <URL>`
captive-portal-page-upload load-file	Loads captive-portal advanced pages
<CAPTIVE-PORTAL-NAME> <URL>	Specify the captive portal's name and location. The captive portal should be existing and configured. • <URL> – Specifies file location in the following format: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>:<passwd>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb<n>:/path/file

Example

```
rfs4000-229D58>captive-portal-page-upload test1 00-04-96-4A-A7-08 upload-time
03/01/2013-12:30
--------------------------------------------------------------------------------
---
        CONTROLLER         STATUS                      MESSAGE
--------------------------------------------------------------------------------
---
  00-23-68-22-9D-58       Fail       Failed to initiate page upload

--------------------------------------------------------------------------------
---
rfs4000-229D58>

rfs4000-229D58>captive-portal-page-upload cancel-upload 00-04-96-4A-A7-08
```

```
-------------------------------------------------------------------------------
---
         CONTROLLER              STATUS                    MESSAGE
-------------------------------------------------------------------------------
---
  00-23-68-22-9D-58         Success         Cancelled upgrade of 1 APs
-------------------------------------------------------------------------------
---
rfs4000-229D58>
```

change-passwd

User Exec Commands

Changes the password of a logged user. When this command is executed without any parameters, the password can be changed interactively.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
change-passwd {<OLD-PASSWORD>} <NEW-PASSWORD>
```

Parameters

```
change-passwd {<OLD-PASSWORD>} <NEW-PASSWORD>
```

<OLD-PASSWORD>	Optional. Specify the password to be changed.
<NEW-PASSWORD>	Specify the new password. **NOTE:** The password can also be changed interactively. To do so, press [**Enter**] after the command.

Usage Guidelines:

A password must be from 1 - 64 characters.

Example

```
rfs7000-37FABE>change-passwd
Enter old password:
Enter new password:
Password for user 'admin' changed successfully
Please write this password change to memory(write memory) to be persistent.
rfs7000-37FABE#write memory
OK
rfs7000-37FABE>
```

clear

User Exec Commands

Clears parameters, cache entries, table entries, and other similar entries. The clear command is available for specific commands only. The information cleared, using this command, depends on the mode where the clear command is executed.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

NOTE
Refer to the interface details below when using clear
- ge <index> – Brocade Mobility RFS4000 supports 5 GEs, Brocade Mobility RFS6000 supports 8 GEs
- me1 – Available in both Brocade Mobility RFS7000 and Brocade Mobility RFS6000
- up1 – Uplink interface on Brocade Mobility RFS4000

Syntax:

```
clear
[arp-cache|cdp|counters|crypto|event-history|gre|ip|lldp|mac-address-table|
          mint|role|rtls|smart-cache|spanning-tree|vrrp]

clear arp-cache {on <DEVICE-NAME>}

clear [cdp|lldp] neighbors {on <DEVICE-NAME>}

clear counters [br|radio|wireless-client]
clear counters [br {<MAC>}|radio {<MAC/DEVICE-NAME>} {<1-3>}|wireless-client
{<MAC>}]
          {(on <DEVICE-OR-DOMAIN-NAME>)}

clear crypto [ike|ipsec] sa
clear crypto ike sa [<IP>|all] {on <DEVICE-NAME>}
clear crypto ipsec sa {on <DEVICE-NAME>}

clear event-history

clear gre stats {on <DEVICE-NAME>}

clear ip [dhcp|ospf]
clear ip dhcp bindings [<IP>|all] {on <DEVICE-NAME>}
clear ip ospf process {on <DEVICE-NAME>}

clear mac-address-table {address|interface|vlan} {on <DEVICE-NAME>}

clear mac-address-table {address <MAC>|vlan <1-4094>} {on <DEVICE-NAME>}
clear mac-address-table interface [<IF-NAME>|ge <1-X>|port-channel <1-X>|
          t1e1 <1-4> <1-1>|up <1-X>|vmif <1-X>|xge <1-4>] {on <DEVICE-NAME>}

clear mint mlcp history {on <DEVICE-NAME>}

clear role ldap-stats {on <DEVICE-NAME>}
```

```
clear rtls [aeroscout|ekahau]
clear rtls [aeroscout|ekahau] {<DEVICE-NAME> {on <DEVICE-OR-DOMAIN-NAME>}|
          on <DEVICE-OR-DOMAIN-NAME>}

clear spanning-tree detected-protocols {interface|on}
clear spanning-tree detected-protocols {on <DEVICE-NAME>}
clear spanning-tree detected-protocols {interface [<INTERFACE-NAME>|ge
<1-5>|me1|
          port-channel <1-3>|pppoe1|up1|vlan <1-4094>|wwan1]} {on
<DEVICE-NAME>}

clear vrrp [error-stats|stats] {on <DEVICE-NAME>}
```

Parameters

`clear arp-cache {on <DEVICE-NAME>}`

arp-cache	Clears *Address Resolution Protocol* (ARP) cache entries on a AP, wireless controller, or service platform. This protocol matches the layer 3 IP addresses to the layer 2 MAC addresses.
on <DEVICE-NAME>	Optional. Clears ARP cache entries on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`clear [cdp|lldp] neighbors {on <DEVICE-NAME>}`

cdp	Clears *Cisco Discovery Protocol* (CDP) table entries
lldp	Clears *Link Layer Discovery Protocol* (LLDP) table entries
neighbors	Clears CDP or LLDP neighbor table entries based on the option selected in the preceding step
on <DEVICE-NAME>	Optional. Clears CDP or LLDP neighbor table entries on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`clear counters [br {<MAC>}|radio {<MAC/DEVICE-NAME>} {<1-3>}|wireless-client {<MAC>}] {(on <DEVICE-OR-DOMAIN-NAME>)}`

counters	Clears counters based on the parameters passed. The options are: AP, radio, and wireless clients.
br <MAC>	Clears counters for all APs or a specified AP • <MAC> – Optional. Specify the AP's MAC address. If no MAC address is specified, all AP counters are cleared.
radio <MAC/DEVICE-NAME> <1-3>	Clears radio interface counters on a specified device or on all devices • <MAC/DEVICE-NAME> – Optional. Specify the device's hostname or MAC address. Optionally, append the radio interface number (to the radio ID) using one of the following formats: AA-BB-CC-DD-EE-FF:RX or HOSTNAME:RX (where RX is the interface number). • <1-3> – Optional. Identifies the radio interface by its index. Specify the radio interface index, if not specified as part of the radio ID. If no device name or MAC address is specified, all radio interface counters are cleared.
wireless-client <MAC>	Clears counters for all wireless clients or a specified wireless client • <MAC> – Optional. Specify the wireless client's MAC address. If no MAC address is specified, all wireless client counters are cleared.
on <DEVICE-OR-DOMAIN-NAME>	This keyword is common to all of the above keywords. • on <DEVICE-OR-DOMAIN-NAME> – Optional. Clears AP, radio, or wireless client counters on a specified AP, wireless controller, service platform, or RF Domain.

clear crypto ike sa [<IP>|all] *{on <DEVICE-NAME>}*	
crypto	Clears encryption module database
ike sa [<IP>|all]	Clears *Internet Key Exchange* (IKE) *security associations* (SAs) • <IP> – Clears IKE SA entries for the peer identified by the <IP> keyword • all – Clears IKE SA entries for all peers
on <DEVICE-NAME>	Optional. Clears IKE SA entries, for a specified peer or all peers, on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

clear crypto ipsec sa *{on <DEVICE-NAME>}*	
crypto	Clears encryption module database
ipsec sa {on <DEVICE-NAME>}	Clears *Internet Protocol Security* (IPSec) database SAs • on <DEVICE-NAME> – Optional. Clears IPSec SA entries on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

clear gre stats *{on <DEVICE-NAME>}*	
gre stats	Clears GRE tunnel statistics
on <DEVICE-NAME>	Optional. GRE tunnel statistics on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

clear event-history	
event-history	Clears event history cache entries

clear ip dhcp bindings [<IP>|all] *{on <DEVICE-NAME>}*	
ip	Clears a *Dynamic Host Configuration Protocol* (DHCP) server's IP address binding entries
dhcp bindings	Clears DHCP connections and server bindings
<IP>	Clears specific address binding entries. Specify the IP address to clear binding entries.
all	Clears all address binding entries
on <DEVICE-NAME>	Optional. Clears a specified address binding or all address bindings on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

clear ip ospf process *{on <DEVICE-NAME>}*	
ip ospf process	Clears already enabled *Open Shortest Path First* (OSPF) process and restarts the process
on <DEVICE-NAME>	Optional. Clears OSPF process on a specified device OSPF is a link-state *interior gateway protocol* (IGP). OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighboring routers and constructs a network topology. The topology determines the routing table presented to the Internet Layer, which makes routing decisions based solely on the destination IP address found in IP packets. • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

clear mac-address-table *{address <MAC>|vlan <1-4094>} {on <DEVICE-NAME>}*	
mac-address-table	Clears the MAC address forwarding table
address <MAC>	Optional. Clears a specified MAC address from the MAC address table. • <MAC> – Specify the MAC address in one of the following formats: AA-BB-CC-DD-EE-FF or AA:BB:CC;DD:EE:FF or AABB.CCDD.EEFF

vlan <1-4094>	Optional. Clears all MAC addresses for a specified VLAN • <1-4094> – Specify the VLAN ID from 1 - 4094
on <DEVICE-NAME>	Optional. Clears a single MAC entry or all MAC entries, for the specified VLAN on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
clear mac-address-table interface [<IF-NAME>|ge <1-X>|port-channel <1-X>|
t1e1 <1-4> <1-1>|up <1-2>|vmif <1-X>|xge <1-4>] {on <DEVICE-NAME>}
```

mac-address-table	Clears the MAC address forwarding table
interface	Clears all MAC addresses for the selected interface. Use the options available to specify the interface.
<IF-NAME>	Clears MAC address forwarding table for the specified layer 2 interface (Ethernet port) • <IF-NAME> – Specify the layer 2 interface name.
ge <1-X>	Clears MAC address forwarding table for the specified GigabitEthernet interface • <1-X> – Specify the GigabitEthernet interface index from 1 - X. The number of Ethernet interfaces supported varies for different device types. Brocade Mobility RFS4000 supports 5 GE interfaces.
port-channel <1-X>	Clears MAC address forwarding table for the specified port-channel interface • <1-X> – Specify the port-channel interface index from 1 - X. The number of port-channel interfaces supported varies for different device types. Brocade Mobility RFS4000 supports 3 port-channels.
t1e1 <1-4> <1-1>	Clears MAC address forwarding table for the specified T1E1L interface • <1-4> – Specify the T1E1 interface index from 1 - 4. A maximum of 4 slots are available. Select the slot to clear the MAC address forwarding table.
up <1-X>	Clears MAC address forwarding table for the WAN Ethernet interface The number of WAN Ethernet interfaces supported varies for different devices. The Brocade Mobility RFS4000 and Brocade Mobility RFS6000 devices support 1 WAN Ethernet interface.
vmif <1-X>	Clears MAC address forwarding table for the VM interface • <1-X> – Specify the VM interface index from 1 - X. The VMIF interfaces are supported only on the Brocade Mobility RFS9510 series service platforms. The number of supported VMIFs varies for different device types.
xge <1-4>	Clears MAC address forwarding table for the specified TenGigabitEthernet interface • <1-4> – Specify the GigabitEthernet interface index from 1 - 4. This interface is supported only on the NX9000 series service platforms.
on <DEVICE-NAME>	Optional. Clears the MAC address forwarding table, for the selected interface, on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
clear mint mlcp history {on <DEVICE-NAME>}
```

mint	Clears MiNT related information
mlcp history	Clears *MiNT Link Creation Protocol* (MLCP) client history
on <DEVICE-NAME>	Optional. Clears MLCP client history on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
clear role ldap-stats {on <DEVICE-NAME>}
```

role ldap-stats	Clears LDAP server statistics
on <DEVICE-NAME>	Optional. Clears LDAP server statistics on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`clear rtls [aeroscout|ekahau] {<DEVICE-NAME> {on <DEVICE-OR-DOMAIN-NAME>}| on <DEVICE-OR-DOMAIN-NAME>}`

rtls	Clears *Real Time Location Service* (RTLS) statistics
aeroscout	Clears RTLS Aeroscout statistics
ekahau	Clears RTLS Ekahau statistics
on <DEVICE-NAME>	This keyword is common to the 'aeroscout' and 'ekahau' parameters. • on <DEVICE-NAME> – Optional. Clears Aeroscout or Ekahau RTLS statistics– AP, wireless controller, or service platform
on <DEVICE-OR-DOMAIN-NAME>	This keyword is common to the 'aeroscout' and 'ekahau' parameters. • on <DEVICE-OR-DOMAIN-NAME> – Optional. Clears Aeroscout or Ekahau RTLS statistics on a specified AP, wireless controller, service platform, or RF Domain

`clear spanning-tree detected-protocols {on <DEVICE-NAME>}`

spanning-tree	Clears spanning tree entries on an interface, and restarts protocol migration
detected-protocols	Restarts protocol migration
on <DEVICE-NAME>	Optional. Clears spanning tree entries on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`clear spanning-tree detected-protocols {interface [<INTERFACE-NAME>|ge <1-5>| me1|port-channel <1-3>|pppoe1|up1|vlan <1-4094>|wwan1]} {on <DEVICE-NAME>}`

spanning-tree	Clears spanning tree entries on an interface and restarts protocol migration
detected-protocols	Restarts protocol migration
interface [<INTERFACE-NAME>| ge <1-5>|me1| port-channel <1-3>| pppoe1|up1| vlan <1-4094>| wwan1]	Optional. Clears spanning tree entries on different interfaces • <INTERFACE-NAME> – Clears detected spanning tree entries on a specified interface. Specify the interface name. • ge <1-5> – Clears detected spanning tree entries for the selected GigabitEthernet interface. Select the GigabitEthernet interface index from 1 - 5. • me1 – Clears FastEthernet interface status • port-channel <1-3> – Clears detected spanning tree entries for the selected port channel interface. Select the port channel index from 1 - 3. • pppoe1 – Clears detected spanning tree entries for *Point-to-Point Protocol over Ethernet* (PPPoE) interface • up1 – Clears detected spanning tree entries for the WAN Ethernet interface • vlan <1-4094> – Clears detected spanning tree entries for the selected VLAN interface. Select a *Switch Virtual Interface* (SVI) VLAN ID from 1- 4094. • wwan1 – Clears detected spanning tree entries for wireless WAN interface.
on <DEVICE-NAME>	Optional. Clears spanning tree entries on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`clear vrrp [error-stats|stats] {on <DEVICE-NAME>}`

vrrp	Clears a device's *Virtual Router Redundancy Protocol* (VRRP) statistics VRRP allows a pool of routers to be advertized as a single virtual router. This virtual router is configured by hosts as their default gateway. VRRP elects a master router, from this pool, and assigns it a virtual IP address. The master router routes and forwards packets to hosts on the same subnet. When the master router fails, one of the backup routers is elected as the master and its IP address is mapped to the virtual IP address.
error-stats	Clears global error statistics

stats	Clears VRRP related statistics
on <DEVICE-NAME>	This following keywords are common to the 'error-stats' and 'stats' parameters: • on <DEVICE-NAME> – Optional. Clears VRRP statistics on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Example

```
rfs4000-229D58>clear event-history

rfs4000-229D58>clear spanning-tree detected-protocols interface port-channel 1
on rfs4000-229D58

rfs4000-229D58>clear spanning-tree detected-protocols interface ge 1

rfs4000-229D58>clear lldp neighbors

rfs4000-229D58>show cdp neighbors
-------------------------------------------------------------------------------
---
     Device ID           Platform        Local Intrfce    Port ID      Duplex
-------------------------------------------------------------------------------
---
 rfs4000-880DA7    RFS-4011-11110-US    ge1              ge1        full
 rfs7000-37FDF2    RFS-7010-1000-WR     ge1              ge1        full
 rfs6000-434CAA    Brocade Mobility RFS6000           ge1            ge1
full
 br7131-139B34    Brocade Mobility 7131 Access PointN           ge1
ge1        full
-------------------------------------------------------------------------------
---rfs4000-229D58>

rfs4000-229D58>clear cdp neighbors

rfs4000-229D58>show cdp neighbors
-------------------------------------------------------------------------------
---
     Device ID         Platform     Local Intrfce      Port ID        Duplex
-------------------------------------------------------------------------------
---

-------------------------------------------------------------------------------
---

rfs4000-229D58>

rfs4000-229D58>clear role ldap-stats

rfs4000-229D58>show role ldap-stats
No ROLE LDAP statistics found.
rfs4000-229D58>

rfs4000-229D58>show mac-address-table
-----------------------------------------------------------
 BRIDGE VLAN PORT             MAC               STATE
-----------------------------------------------------------
 1      1    ge5              00-02-B3-28-D1-55 forward
 1      1    ge5              00-0F-8F-19-BA-4C forward
 1      1    ge5              B4-C7-99-5C-FA-8E forward
```

```
 1      1    ge5              00-23-68-0F-43-D8 forward
 1      1    ge5              00-15-70-38-06-49 forward
 1      1    ge5              00-23-68-13-9B-34 forward
 1      1    ge5              B4-C7-99-58-72-58 forward
 1      1    ge5              00-15-70-81-74-2D forward
 1      1    ge5              B4-C7-99-5C-FA-2B forward
 1      1    ge5              00-15-70-37-FD-F2 forward
 1      1    ge5              B4-C7-99-6C-88-09 forward
 1      1    ge5              B4-C7-99-71-17-28 forward
 1      1    ge5              5C-0E-8B-18-10-91 forward
 1      1    ge5              3C-CE-73-F4-47-83 forward
 1      1    ge5              00-23-68-88-0D-AC forward
 1      1    ge5              00-A0-F8-68-D5-5C forward
-------------------------------------------------------
Total number of MACs displayed: 16
rfs4000-229D58>

rfs4000-229D58>clear mac-address-table address 00-02-B3-28-D1-55 on
rfs4000-229D58

In the following example the first MAC address in the table has been cleared.
Now the table has only 15 entries.

rfs4000-229D58>show mac-address-table on rfs4000-229D58
-------------------------------------------------------
 BRIDGE VLAN PORT             MAC               STATE
-------------------------------------------------------
 1      1    ge5              00-0F-8F-19-BA-4C forward
 1      1    ge5              B4-C7-99-5C-FA-8E forward
 1      1    ge5              00-23-68-0F-43-D8 forward
 1      1    ge5              00-15-70-38-06-49 forward
 1      1    ge5              00-23-68-13-9B-34 forward
 1      1    ge5              B4-C7-99-58-72-58 forward
 1      1    ge5              00-15-70-81-74-2D forward
 1      1    ge5              B4-C7-99-5C-FA-2B forward
 1      1    ge5              00-15-70-37-FD-F2 forward
 1      1    ge5              B4-C7-99-6C-88-09 forward
 1      1    ge5              B4-C7-99-71-17-28 forward
 1      1    ge5              5C-0E-8B-18-10-91 forward
 1      1    ge5              3C-CE-73-F4-47-83 forward
 1      1    ge5              00-23-68-88-0D-AC forward
 1      1    ge5              00-A0-F8-68-D5-5C forward
-------------------------------------------------------
Total number of MACs displayed: 15
rfs4000-229D58>
```

clock

User Exec Commands

Sets a device's system clock

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
clock set <HH:MM:SS> <1-31> <MONTH> <1993-2035> {on <DEVICE-NAME>}
```

Parameters

```
clock set <HH:MM:SS> <1-31> <MONTH> <1993-2035> {on <DEVICE-NAME>}
```

clock set	Sets a device's software system clock
<HH:MM:SS>	Sets the current time (in military format hours, minutes and seconds)
<1-31>	Sets the numerical day of the month
<MONTH>	Sets the month of the year (Jan to Dec)
<1993-2035>	Sets a valid four digit year from 1993 - 2035
on <DEVICE-NAME>	Optional. Sets the clock on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Example

```
rfs4000-229D58>clock set 14:25:35 15 Feb 2013

rfs4000-229D58>show clock
2013-02-15 14:25:40 UTC
rfs4000-229D58>
```

cluster

User Exec Commands

Initiates cluster context. The cluster context provides centralized management to configure all cluster members from any one member.

Commands executed under this context are executed on all members of the cluster.

Supported in the following platforms:

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
cluster start-election
```

Parameters

```
cluster start-election
```

start-election	Starts a new cluster master election

Example

```
rfs7000-37FABE>cluster start-election
rfs7000-37FABE>
```

Related Commands:

create-cluster	Creates a new cluster on the specified device
join-cluster	Adds a wireless controller or service platform, as a member, to an existing cluster of controllers

connect

User Exec Commands

Begins a console connection to a remote device using the remote device's MiNT ID or name

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
connect [mint-id <MINT-ID>|<REMOTE-DEVICE-NAME>]
```

Parameters

```
connect [mint-id <MINT-ID>|<REMOTE-DEVICE-NAME>]
```

mint-id <MINT-ID>	Connects to the remote system using its MiNT ID • <MINT-ID> – Specify the remote device's MiNT ID.
<REMOTE-DEVICE-NAME>	Connects to the remote system using its name • <REMOTE-DEVICE-NAME> – Specify the remote device's name.

Example

```
rfs7000-37FABE>show mint lsp-db
2 LSPs in LSP-db of 70.37.FA.BE:
LSP 68.11.E6.C4 at level 1, hostname "ap7131-11E6C4", 1 adjacencies, seqnum
LSP 70.37.FA.BE at level 1, hostname "rfs7000-37FABE", 1 adjacencies, seqnu20
rfs7000-37FABE>connect mint-id 68.11.E6.C4 ?

Entering character mode
Escape character is '^

rfs7000-37FABE>connect mint-id 68.11.E6.C4 ?

Entering character mode
Escape character is '^]'.

Brocade Mobility 7131 Access Point release 5.5.0.0-018D
br7131-11E6C4 login: Connection closed by foreign host
rfs7000-37FABE>

rfs4000-229D58>show mint lsp-db
1 LSPs in LSP-db of 68.22.9D.58:
LSP 68.22.9D.58 at level 1, hostname "rfs4000-229D58", 0 adjacencies, seqnum
606
```

```
rfs4000-229D58>

rfs4000-229D58>connect ?
  REMOTE-DEVICE-NAME  Name of remote system
  mint-id             MiNT protocol identifier

rfs4000-229D58>connect mint-id 68.22.9D.58

Entering character mode
Escape character is '^]'.

Brocade Mobility RFS4000 release 5.5.0.0-018D
rfs4000-229D58 login:
```

create-cluster

User Exec Commands

Creates a new device cluster with the specified name and assigns it an IP address and routing level

A cluster (or redundancy group) is a set of controllers or service platforms (nodes) uniquely defined by a profile configuration. Within the cluster, members discover and establish connections to other members and provide wireless network self-healing support in the event of member's failure.

A cluster's load balance is typically distributed evenly amongst its members. An administrator needs to define how often the profile is load balanced for radio distribution, as radios can come and go and members join and exit the cluster.

Supported in the following platforms:

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
create-cluster name <CLUSTER-NAME> ip <IP> {level [1|2]}
```

Parameters

```
create-cluster name <CLUSTER-NAME> ip <IP> {level [1|2]}
```

create-cluster	Creates a cluster
name <CLUSTER-NAME>	Configures the cluster name • <CLUSTER-NAME> – Specify a cluster name. Define a name for the cluster name unique to its configuration or profile support requirements. The name cannot exceed 64 characters.
ip <IP>	Specifies the device's IP address used for cluster creation • <IP> – Specify the device's IP address in the A.B.C.D format.
level [1|2]	Optional. Configures the cluster's routing level • 1 – Configures level 1 (local) routing • 2 – Configures level 2 (inter-site) routing

Example

```
rfs7000-37FABE>create-cluster name Cluster1 ip 172.16.10.1 level 1
... creating cluster
... committing the changes
... saving the changes
```

```
[OK]
rfs7000-37FABE>

nx6500-31FABE>create-cluster <CLUSTER-NAME>
```

Related Commands:

cluster	Initiates cluster context. The cluster context provides centralized management to configure all cluster members from any one member.
join-cluster	Adds a device, as a member, to an existing cluster of devices

crypto

User Exec Commands

Enables digital certificate configuration and RSA Keypair management. Digital certificates are issued by CAs and contain user or device specific information, such as name, public key, IP address, serial number, company name etc. Use this command to generate, delete, export, or import encrypted RSA Keypairs and generate *Certificate Signing Request* (CSR).

This command also enables trustpoint configuration. Trustpoints contain the CA's identity and configuration parameters.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
crypto [key|pki]

crypto key [export|generate|import|zeroize]

crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL>
{background|on|passphrase}
crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL>
          {background {on <DEVICE-NAME>}|on <DEVICE-NAME>}
crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL>
          {passphrase <KEY-PASSPHRASE> {background {on <DEVICE-NAME>}|on
<DEVICE-NAME>}}

crypto key generate rsa <RSA-KEYPAIR-NAME> <1024-2048> {on <DEVICE-NAME>}

crypto key import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL>
{background|on|passphrase}
crypto key import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL>
          {background {on <DEVICE-NAME>}|on <DEVICE-NAME>}
crypto key import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL>
          {passphrase <KEY-PASSPHRASE> {background {on <DEVICE-NAME>}|on
<DEVICE-NAME>}}
```

```
crypto key zeroize rsa <RSA-KEYPAIR-NAME> {force {on <DEVICE-NAME>}|on
<DEVICE-NAME>}

crypto pki [authenticate|export|generate|import|zeroize]

crypto pki authenticate <TRUSTPOINT-NAME> <LOCATION-URL>
          {background {on <DEVICE-NAME>}|on <DEVICE-NAME>}

crypto pki export [request|trustpoint]
crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME>
          [autogen-subject-name|subject-name]
crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME>
   autogen-subject-name (<EXPORT-TO-URL>,email <SEND-TO-EMAIL>,fqdn <FQDN>,
   ip-address <IP>)
crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME>
   autogen-subject-name <EXPORT-TO-URL> {background {on <DEVICE-NAME>}|
   on <DEVICE-NAME>}
crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME>
          subject-name <COMMON-NAME> <COUNTRY> <STATE> <CITY> <ORGANIZATION>
   <ORGANIZATION-UNIT> (<EXPORT-TO-URL>,email <SEND-TO-EMAIL>,fqdn <FQDN>,
   ip-address <IP>)

crypto pki export trustpoint <TRUSTPOINT-NAME> <EXPORT-TO-URL> {background
  {on <DEVICE-NAME>}|on <DEVICE-NAME>|passphrase <KEY-PASSPHRASE> {background
  {on <DEVICE-NAME>}|on <DEVICE-NAME>}}

crypto pki generate self-signed <TRUSTPOINT-NAME> [generate-rsa-key|
  use-rsa-key] <RSA-KEYPAIR-NAME> [autogen-subject-name|subject-name]
crypto pki generate self-signed <TRUSTPOINT-NAME> [generate-rsa-key|
  use-rsa-key] <RSA-KEYPAIR-NAME> autogen-subject-name {(email
<SEND-TO-EMAIL>,
  fqdn <FQDN>,ip-address <IP>,on <DEVICE-NAME>)}
crypto pki generate self-signed <TRUSTPOINT-NAME> [generate-rsa-key|
  use-rsa-key] <WORD> subject-name <COMMON-NAME> <COUNTRY> <STATE> <CITY>
  <ORGANIZATION> <ORGANIZATION-UNIT> {(email <SEND-TO-EMAIL>,fqdn <FQDN>,
  ip-address <IP>,on <DEVICE-NAME>)}

crypto pki import [certificate|crl|trustpoint]
crypto pki import [certificate|crl] <TRUSTPOINT-NAME> <IMPORT-FROM-URL>
  {background {on <DEVICE-NAME>}|on <DEVICE-NAME>}]
crypto pki import trustpoint <TRUSTPOINT-NAME> <IMPORT-FROM-URL>
  {background {on <DEVICE-NAME>}|on <DEVICE-NAME>|passphrase <KEY-PASSPHRASE>
  {background {on <DEVICE-NAME>}|on <DEVICE-NAME>}}

crypto pki zeroize trustpoint <TRUSTPOINT-NAME> {del-key {on <DEVICE-NAME>}|
  on <DEVICE-NAME>}
```

Parameters

```
crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL>
{background {on <DEVICE-NAME>}|on <DEVICE-NAME>}
```

key	Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.
export rsa <RSA-KEYPAIR-NAME>	Exports an existing RSA Keypair to a specified destination • <RSA-KEYPAIR-NAME> – Specify the RSA Keypair name.

<EXPORT-TO-URL>	Specify the RSA Keypair destination address in the following format: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb<n>:/path/file
background {on <DEVICE-NAME>}	Optional. Performs export operation in the background. Optionally specify the device to perform export on.
on <DEVICE-NAME>	Optional. Performs export operation on a specific device. • on <DEVICE-NAME> – Optional. Performs export operation on a specific device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL>
{passphrase <KEY-PASSPHRASE> {background {on <DEVICE-NAME>}|on <DEVICE-NAME>}}
```

key	Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.
export rsa	Exports a RSA Keypair to a specified destination • <RSA-KEYPAIR-NAME> – Specify the RSA Keypair name.
<EXPORT-TO-URL> {passphrase <KEY-PASSPHRASE>}	Specify the RSA Keypair destination address in the following format: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb<n>:/path/file • passphrase – Optional. Encrypts RSA Keypair before exporting it • <KEY-PASSPHRASE> – Specify a passphrase to encrypt the RSA Keypair.
on <DEVICE-NAME>	Optional. Performs export operation on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
crypto key generate rsa <RSA-KEYPAIR-NAME> <1024-2048> {on <DEVICE-NAME>}
```

key	Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.
generate rsa <RSA-KEYPAIR-NAME> <1024-2048>	Generates a new RSA Keypair • <RSA-KEYPAIR-NAME> – Specify the RSA Keypair name. • <1024-2048> – Sets the size of the RSA key in bits from 1024 - 2048. The default size is 1024.
on <DEVICE-NAME>	Optional. Generates the new RSA Keypair on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
crypto key import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL>
{background {on <DEVICE-NAME>}|on <DEVICE-NAME>}
```

key	Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.
import rsa <RSA-KEYPAIR-NAME>	Imports a RSA Keypair from a specified source • <RSA-KEYPAIR-NAME> – Specify the RSA Keypair name.

<IMPORT-FROM-URL>	Specify the RSA Keypair source address in the following format: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb<n>:/path/file
on <DEVICE-NAME>	Optional. Performs import operation on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.
background {on <DEVICE-NAME>}	Optional. Performs import operation in the background • on <DEVICE-NAME> – Optional. Performs import operation on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`crypto key import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL> {passphrase <KEY-PASSPHRASE> {background {on <DEVICE-NAME>}|on <DEVICE-NAME>}}`

key	Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.
import rsa <RSA-KEYPAIR-NAME>	Decrypts and imports a RSA Keypair from a specified source • <RSA-KEYPAIR-NAME> – Specify the RSA Keypair name.
<IMPORT-FROM-URL> {passphrase <KEY-PASSPHRASE>}	Specify the RSA Keypair source address in the following format: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb<n>:/path/file • passphrase – Optional. Decrypts the RSA Keypair before importing it • <KEY-PASSPHRASE> – Specify the passphrase to decrypt the RSA Keypair.
on <DEVICE-NAME>	Optional. Performs import operation on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`crypto key zeroize <RSA-KEYPAIR-NAME> {force {on <DEVICE-NAME>}|on <DEVICE-NAME>}`

key	Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.
zeroize rsa <RSA-KEYPAIR-NAME>	Deletes a specified RSA Keypair • <RSA-KEYPAIR-NAME> – Specify the RSA Keypair name. **NOTE:** All device certificates associated with this key will also be deleted.
force {on <DEVICE-NAME>}	Optional. Forces deletion of all certificates associated with the specified RSA Keypair. Optionally specify a device on which to force certificate deletion.
on <DEVICE-NAME>	Optional. Deletes all certificates associated with the RSA Keypair on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`crypto pki authenticate <TRUSTPOINT-NAME> <URL> {background {on <DEVICE-NAME>}| on <DEVICE-NAME>}`

pki	Enables *Private Key Infrastructure* (PKI) management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated *Certificate Authority* (CA) certificates.
authenticate <TRUSTPOINT-NAME>	Authenticates a trustpoint and imports the corresponding CA certificate • <TRUSTPOINT-NAME> – Specify the trustpoint name.

<URL>	Specify CA's location in the following format: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb<n>:/path/file **NOTE:** The CA certificate is imported from the specified location.
background {on <DEVICE-NAME>}	Optional. Performs authentication in the background. Optionally specify a device on which to perform authentication.
on <DEVICE-NAME>	Optional. Performs authentication on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME>
autogen-subject-name (<EXPORT-TO-URL>,email <SEND-TO-EMAIL>,fqdn
<FQDN>,ip-address <IP>)
```

pki	Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.
export request	Exports CSR to the CA for digital identity certificate. The CSR contains applicant's details and RSA Keypair's public key.
[generate-rsa-key| use-rsa-key] <RSA-KEYPAIR-NAME>	Generates a new RSA Keypair or uses an existing RSA Keypair • generate-rsa-key – Generates a new RSA Keypair for digital authentication • use-rsa-key – Uses an existing RSA Keypair for digital authentication • <RSA-KEYPAIR-NAME> – If generating a new RSA Keypair, specify a name for it. If using an existing RSA Keypair, specify its name.
autogen-subject-name	Auto generates subject name from configuration parameters. The subject name identifies the certificate.
<EXPORT-TO-URL> {background {on <DEVICE-NAME}| on <DEVICE-NAME>}	Specify the CA's location in the following format: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb<n>:/path/file **NOTE:** The CSR is exported to the specified location. • background – Optional. Performs export operation in the background • on <DEVICE-NAME> – Optional. Performs export operation on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.
email <SEND-TO-EMAIL>	Exports CSR to a specified e-mail address • <SEND-TO-EMAIL> – Specify the CA's e-mail address.
fqdn <FQDN>	Exports CSR to a specified *Fully Qualified Domain Name* (FQDN) • <FQDN> – Specify the CA's FQDN.
ip address <IP>	Exports CSR to a specified device or system • <IP> – Specify the CA's IP address.

	`crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME> subject-name <COUNTRY> <STATE> <CITY> <ORGANIZATION> <ORGANIZATION-UNIT> (<EXPORT-TO-URL>,email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address <IP>)`
pki	Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.
export request	Exports CSR to the CA for a digital identity certificate.The CSR contains applicant's details and RSA Keypair's public key.
[generate-rsa-key| use-rsa-key] <RSA-KEYPAIR-NAME>	Generates a new RSA Keypair or uses an existing RSA Keypair • generate-rsa-key – Generates a new RSA Keypair for digital authentication • use-rsa-key – Uses an existing RSA Keypair for digital authentication • <RSA-KEYPAIR-NAME> – If generating a new RSA Keypair, specify a name for it. If using an existing RSA Keypair, specify its name.
subject-name <COMMON-NAME>	Specifies subject name to identify the certificate • <COMMON-NAME> – Sets the common name used with the CA certificate. The name should enable you to identify the certificate easily (2 to 64 characters in length).
<COUNTRY>	Sets the deployment country code (2 character ISO code)
<STATE>	Sets the state name (2 to 64 characters in length)
<CITY>	Sets the city name (2 to 64 characters in length)
<ORGANIZATION>	Sets the organization name (2 to 64 characters in length)
<ORGANIZATION-UNIT>	Sets the organization unit (2 to 64 characters in length)
<EXPORT-TO-URL> {background {on <DEVICE-NAME}| on <DEVICE-NAME>}	Specify the CA's location in the following format: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb<n>:/path/file **NOTE:** The CSR is exported to the specified location. • background – Optional. Performs export operation in the background • on <DEVICE-NAME> – Optional. Performs export operation on a specific device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.
email <SEND-TO-EMAIL>	Exports CSR to a specified e-mail address • <SEND-TO-EMAIL> – Specify the CA's e-mail address.
fqdn <FQDN>	Exports CSR to a specified FQDN • <FQDN> – Specify the CA's FQDN.
ip address <IP>	Exports CSR to a specified device or system • <IP> – Specify the CA's IP address.

	`crypto pki export trustpoint <TRUSTPOINT-NAME> <EXPORT-TO-URL> {background {on <DEVICE-NAME>}|on <DEVICE-NAME>|passphrase <KEY-PASSPHRASE> background {on <DEVICE-NAME>}|on <DEVICE-NAME>}}`
pki	Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.
export trustpoint <TRUSTPOINT-NAME>	Exports a trustpoint along with CA certificate, *Certificate Revocation List* (CRL), server certificate, and private key • <TRUSTPOINT-NAME> – Specify the trustpoint name.

<EXPORT-TO-URL>	Specify the destination address in the following format: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb<n>:/path/file
background {on <DEVICE-NAME>}	Optional. Performs export operation in the background • on <DEVICE-NAME> – Optional. Performs export operation on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.
on <DEVICE-NAME>	Optional. Performs export operation on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.
passphrase <KEY-PASSPHRASE> {background {on <DEVICE-NAME>}| on <DEVICE-NAME>}	Optional. Encrypts the key with a passphrase before exporting it • <KEY-PASSPHRASE> – Specify the passphrase. • background – Optional. Performs export operation in the background • on <DEVICE-NAME> – Optional. Performs export operation on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`crypto pki generate self-signed <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME> autogen-subject-name {(email <SEND-TO-EMAIL>, fqdn <FQDN>, ip-address <IP>, on <DEVICE-NAME>)}`

pki	Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.
generate	Generates a CA certificate and a trustpoint
self-signed <TRUSTPOINT-NAME>	Generates a self-signed CA certificate and a trustpoint • <TRUSTPOINT-NAME> – Specify a name for the certificate and its trustpoint.
[generate-rsa-key| use-rsa-key] <RSA-KEYPAIR-NAME>	Generates a new RSA Keypair, or uses an existing RSA Keypair • generate-rsa-key – Generates a new RSA Keypair for digital authentication • use-rsa-key – Uses an existing RSA Keypair for digital authentication • <RSA-KEYPAIR-NAME> – If generating a new RSA Keypair, specify a name for it. If using an existing RSA Keypair, specify its name.
autogen-subject-name	Auto generates the subject name from the configuration parameters. The subject name helps to identify the certificate
email <SEND-TO-EMAIL>	Optional. Exports CSR to a specified e-mail address • <SEND-TO-EMAIL> – Specify the CA's e-mail address.
fqdn <FQDN>	Optional. Exports CSR to a specified FQDN • <FQDN> – Specify the CA's FQDN.
ip-address <IP>	Optional. Exports CSR to a specified device or system • <IP> – Specify the CA's IP address.
on <DEVICE-NAME>	Optional. Exports the CSR on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
crypto pki generate self-signed <TRUSTPOINT-NAME>
[generate-rsa-key|use-rsa-key]
<RSA-KEYPAIR-NAME> subject-name <COMMON-NAME> <COUNTRY> <STATE> <CITY>
<ORGANIZATION> <ORGANIZATION-UNIT> {(email <SEND-TO-EMAIL>,fqdn
<FQDN>,ip-address <IP>,on <DEVICE-NAME>)}
```

pki	Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.
generate self-signed <TRUSTPOINT-NAME>	Generates a self-signed CA certificate and a trustpoint • <TRUSTPOINT-NAME> – Specify a name for the certificate and its trustpoint.
[generate-rsa-key| use-rsa-key] <RSA-KEYPAIR-NAME>	Generates a new RSA Keypair, or uses an existing RSA Keypair • generate-rsa-key – Generates a new RSA Keypair for digital authentication • use-rsa-key – Uses an existing RSA Keypair for digital authentication • <RSA-KEYPAIR-NAME> – If generating a new RSA Keypair, specify a name for it. If using an existing RSA Keypair, specify its name.
subject-name <COMMON-NAME>	Specify a subject name to identify the certificate. • <COMMON-NAME> – Specify the common name used with the CA certificate. The name should enable you to identify the certificate easily.
<COUNTRY>	Sets the deployment country code (2 character ISO code)
<STATE>	Sets the state name (2 to 64 characters in length)
<CITY>	Sets the city name (2 to 64 characters in length)
<ORGANIZATION>	Sets the organization name (2 to 64 characters in length)
<ORGANIZATION-UNIT>	Sets the organization unit (2 to 64 characters in length)
email <SEND-TO-EMAIL>	Optional. Exports the CSR to a specified e-mail address • <SEND-TO-EMAIL> – Specify the CA's e-mail address.
fqdn <FQDN>	Optional. Exports the CSR to a specified FQDN • <FQDN> – Specify the CA's FQDN.
ip address <IP>	Optional. Exports the CSR to a specified device or system • <IP> – Specify the CA's IP address.

```
crypto pki import [certificate|crl] <TRUSTPOINT-NAME> <IMPORT-FROM-URL>
{background {on <DEVICE-NAME>}|on <DEVICE--NAME>}
```

pki	Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.
import	Imports certificates, *Certificate Revocation List* (CRL), or a trustpoint to the selected device
[certificate|crl] <TRUSTPOINT-NAME>	Imports a signed server certificate or CRL • certificate – Imports signed server certificate • crl – Imports CRL • <TRUSTPOINT-NAME> – Specify the trustpoint name (should be authenticated).
<IMPORT-FROM-URL>	Specify the signed server certificate or CRL source address in the following format: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb<n>:/path/file

background {on <DEVICE-NAME>}	Optional. Performs import operation in the background • on <DEVICE-NAME> – Optional. Performs import operation on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.
on <DEVICE-NAME>	Optional. Performs import operation on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
crypto pki import trustpoint <TRUSTPOINT-NAME> <IMPORT-FROM-URL>
{background {on <DEVICE-NAME>}|on <DEVICE-NAME>|passphrase <KEY-PASSPHRASE>
{background {on <DEVICE-NAME>}|on <DEVICE-NAME>}}
```

pki	Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.
import	Imports certificates, CRL, or a trustpoint to the selected device
trustpoint <TRUSTPOINT-NAME>	Imports a trustpoint and its associated CA certificate, server certificate, and private key • <TRUSTPOINT-NAME> – Specify the trustpoint name (should be authenticated).
<IMPORT-FROM-URL>	Specify the trustpoint source address in the following format: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb<n>:/path/file
background {on <DEVICE-NAME>}	Optional. Performs import operation in the background • on <DEVICE-NAME> – Optional. Performs import operation on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.
on <DEVICE-NAME>	Optional. Performs import operation on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.
passphrase <KEY-PASSPHRASE> {background {on <DEVICE-NAME>}| on <DEVICE-NAME>}	Optional. Encrypts trustpoint with a passphrase before importing it • <KEY-PASSPHRASE> – Specify a passphrase. • background – Optional. Imports the encrypted trustpoint in the background • on <DEVICE-NAME> – Optional. Imports the encrypted trustpoint on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
crypto pki zeroize trustpoint <TRUSTPOINT-NAME> {del-key {on <DEVICE-NAME>}|
on <DEVICE-NAME>}
```

pki	Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.
zeroize <TRUSTPOINT-NAME>	Deletes a trustpoint and its associated CA certificate, server certificate, and private key • <TRUSTPOINT-NAME> – Specify the trustpoint name (should be authenticated).
del-key {on <DEVICE-NAME>}	Optional. Deletes the private key associated with the server certificate • on <DEVICE-NAME> – Optional. Deletes private key on a specific device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.
on <DEVICE-NAME>	Optional. Deletes the trustpoint on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Example

```
rfs7000-37FABE>crypto key generate rsa key 1025
RSA Keypair successfully generated
rfs7000-37FABE>
```

```
rfs7000-37FABE>crypto key import rsa moto123 url passphrase word background on
rfs7000-37FABE
RSA key import operation is started in background
rfs7000-37FABE>

rfs7000-37FABE>crypto pki generate self-signed word generate-rsa-key word
autogen-subject-name fqdn word
Successfully generated self-signed certificate
rfs7000-37FABE>

rfs7000-37FABE>crypto pki zeroize trustpoint word del-key on rfs7000-37FABE
Successfully removed the trustpoint and associated certificates
%Warning: Applications associated with the trustpoint will start using
default-trustpoint
rfs7000-37FABE>

rfs7000-37FABE>crypto pki authenticate word url background on rfs7000-37FABE
Import of CA certificate started in background
rfs7000-37FABE#>

rfs7000-37FABE>crypto pki import trustpoint word url passphrase word on
rfs7000-37FABE
Import operation started in background
rfs7000-37FABE>
```

Related Commands:

no	Removes server certificates, trustpoints and their associated certificates

device-upgrade

User Exec Commands

Enables firmware upgrade on an adopted device or a set of adopted devices (access points, wireless controllers, and service platforms)

In an *hierarchically managed* (HM) network, this command enables centralized device upgradation across the network.

The Mobility HM network defines a three-tier structure, consisting of multiple wireless sites managed by a single *Network Operations Center* (NOC) controller, The NOC controller constitutes the first and the site controllers constitute the second tier of the hierarchy. The site controllers may or may not be grouped to form clusters. The site controllers in turn adopt and manage access points that form the third tier of the hierarchy.

NOTE
Hierarchical management allows the NOC controller to upgrade controllers and access points that are directly or indirectly adopted to it. However, ensure that the NOC controller is loaded with the correct firmware version.

All adopted devices (access points and second-level controllers) are referred to as the ‘adoptee’. The adopting devices are the ‘adopters’. A controller cannot be configured as an adoptee and an adopter simultaneously. In other words, a controller can either be an adopter (adopts another controller) or an adoptee (is adopted by another controller).

Network administrators can use the device-upgrade command to schedule firmware upgrades across adopted devices within the network. Devices are upgraded based on their device names, MAC addresses, or RF Domain. The firmware image used for the upgrade can either be user-defined or built-in.

The user-defined image is pulled from the defined location and applied to the device(s). Use the *device-upgrade* > *load-image* command to provide the image file name and location. User-defined images always get precedence over built-in images.

NOC and site controllers possess built-in firmware images for the various device types. If the administrator has not specified an image file name and location, the image on the controller is used to upgrade the device. The following example describes the various scenarios possible in the absence of a user-defined image.

A site controller has been scheduled to upgrade all adopted APs. Before executing the upgrade, the site controller compares the image it possesses with the image on the NOC controller. In case of an image version mismatch, the site controller does the following:

1. If the site controller is a cluster member, it pulls the image:
    - From a cluster peer, provided the AP image version on the peer and the NOC controller matches.
    - From the NOC controller, if the AP image version on the peer and the NOC controller are mismatched.
    - From the NOC controller, if none of the cluster members possess a AP image.
2. If the site controller is not a cluster member, it pulls the image from the NOC controller.

When upgrading devices in a RF Domain, the process is controlled and driven by the NOC controller. For example, in case of a scheduled upgrading of all APs within an *RF Domain*, the NOC controller:

1. Adopts all controllers, in the RF Domain, to the NOC cluster and gets the status of each controller.
2. Upgrades all controllers, in the cluster, without rebooting them.

    Once the upgrade is completed, the following two scenarios are possible:

    Scenario 1: *If the upgrade/reboot options ARE NOT specified by the network administrator, the NOC controller:*

    a. Pushes the AP image on to the RF Domain manager.

    b. Reboots the active controller within the RF Domain.

    c. Reboots standby controllers after the active controller has successfully rebooted.

    If the controllers are auto upgrade enabled, all APs are upgraded after the controllers have rebooted and the APs have been re-adopted.

    Scenario 2: *If the upgrade/reboot options ARE specified by the network administrator, the NOC controller:*

    a. Reboots the active controller followed by the standby controllers.

    b. Pushes the AP image file on to the RF Domain manager.

    c. Initiates upgrades on all AP within the RF Domain.

    Ensure the RF Domain controllers are auto upgrade enabled.

NOTE
If the *persist-images* option is selected, the RF Domain manager retains the old firmware image, or else deletes it. For more information on enabling device upgrade on profiles and devices (including the 'persist-images' option), see *device-upgrade*.

NOTE
A NOC controller's capacity is equal to, or higher, than that of a site controller. The following devices can be deployed at NOC and sites:
- NOC controller – Brocade Mobility RFS7000 and Brocade Mobility RFS9510)
- Site controller – Brocade Mobility RFS4000, Brocade Mobility RFS6000, and Brocade Mobility RFS7000
Within a HM network, the devices deployed as site controllers depends on the NOC controller device type. For more information on the adoption capabilities of various NOC controller devices, see Usage Guidelines *(NOC controller adoption matrix)*.

NOTE
Standalone devices have to be manually upgraded.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
device-upgrade
[<MAC/HOSTNAME>|all|br650|br6511|br1220|br71xx|br81xx|rfs4000|rfs6000|rfs7000
|cancel-upgrade|load-image|rf-domain]

device-upgrade <MAC/HOSTNAME> {no-reboot|reboot-time <TIME>|
          upgrade-time <TIME> {no-reboot|reboot-time <TIME>}}

device-upgrade all {no-reboot|reboot-time <TIME>|upgrade-time <TIME>
{no-reboot|
          reboot-time <TIME>}} {(staggered-reboot)}

device-upgrade [br650|br6511|br1220|br71xx|br81xx|
          |rfs4000|rfs6000|rfs7000] all
          {no-reboot|reboot-time <TIME>|upgrade-time <TIME>
{no-reboot|reboot-time <TIME>}}
          {(staggered-reboot)}

device-upgrade cancel-upgrade [<MAC/HOSTNAME>|all|br650|br6511|
          br1220|br71xx|br81xx|rfs4000|rfs6000|rfs7000|on]

device-upgrade cancel-upgrade [<MAC/HOSTNAME>|all]

device-upgrade cancel-upgrade [br650|br6511|br1220|
          br71xx|br81xx|rfs4000|rfs6000|rfs7000] all
device-upgrade cancel-upgrade on rf-domain [<RF-DOMAIN-NAME>|all]
```

```
device-upgrade load-image [br650|br6511|br1220|
          br71xx|br81xx|rfs4000|rfs6000|rfs7000] <IMAGE-URL>

device-upgrade rf-domain [<RF-DOMAIN-NAME>|all]
[all|br650|br6511|br1220|br71xx|br81xx|rfs4000|rfs6000|rfs7000]
{<MAC/HOSTNAME>|no-reboot|from-controller|reboot-time <TIME>|
          staggered-reboot|upgrade-time <TIME>}

device-upgrade rf-domain [<RF-DOMAIN-NAME>|all] [all|br650|br6511|br1220|
          br71xx|br81xx|rfs4000|rfs6000|rfs7000]
{<MAC/HOSTNAME>|no-reboot|reboot-time <TIME>} {(staggered-reboot)}

device-upgrade rf-domain [<RF-DOMAIN-NAME>|all] [all|br650|br6511
|br71xx|br81xx|rfs4000|rfs6000|rfs7000]
          {from-controller {no-reboot|reboot-time <TIME>|upgrade-time <TIME>
          {no-reboot|reboot-time <TIME>}} {(staggered-reboot)}

device-upgrade rf-domain [<RF-DOMAIN-NAME>|all] [all|br650|br6511|
          br1220|br71xx|br81xx|rfs4000|rfs6000|rfs7000] {upgrade-time <TIME>
{no-reboot|reboot-time <TIME>}} {(staggered-reboot)}
```

Parameters

```
device-upgrade <MAC/HOSTNAME> {no-reboot|reboot-time <TIME>|upgrade-time
<TIME>
{no-reboot|reboot-time <TIME>}}
```

<MAC/HOSTNAME>	Upgrades firmware on the device identified by the <MAC/HOSTNAME> keyword • <MAC/HOSTNAME> – Specify the device's MAC address or hostname.
no-reboot	Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)
reboot-time <TIME>	Optional. Schedules an automatic reboot after a successful upgrade • <TIME> – Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.
upgrade-time <TIME> {no-reboot| reboot-time <TIME>}	Optional. Schedules an automatic device firmware upgrade • <TIME> – Specify the upgrade time in the MM/DD/YYYY-HH:MM or HH:MM format. The following actions can be performed after a scheduled upgrade: • no-reboot – Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted) • reboot-time <TIME> – Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.

```
device-upgrade all {no-reboot|reboot-time <TIME>|upgrade-time <TIME>
{no-reboot|
reboot-time <TIME>}} {(staggered-reboot)}
```

all	Upgrades firmware on all devices
no-reboot	Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)
reboot-time <TIME>	Optional. Schedules an automatic reboot after a successful upgrade • <TIME> – Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.

upgrade-time <TIME> {no-reboot| reboot-time <TIME>}	Optional. Schedules an automatic device firmware upgrade on all devices • <TIME> – Specify the upgrade time in the MM/DD/YYYY-HH:MM or HH:MM format. The following actions can be performed after a scheduled upgrade: • no-reboot – Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted) • reboot-time <TIME> – Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.
staggered-reboot	This keyword is common to all of the above. • Optional. Enables staggered reboot (one at a time), without network impact

`device-upgrade [br650|br6511|br1220|br71xx|br81xx| |rfs4000|rfs6000|rfs7000] all` *`{no-reboot|reboot-time <TIME>| upgrade-time <TIME> {no-reboot|reboot-time <TIME>}} {(staggered-reboot)}`*

[br650| br6511|br1220| br71xx| br81xx|rfs4000| rfs6000|rfs7000] all	Upgrades firmware on all devices of a specific type. Select the device type. • Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point • Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000 • Service Platforms — Brocade Mobility RFS9510 • all – Upgrades firmware on all • Brocade Mobility 650 Access Point all – Upgrades firmware on all Brocade Mobility 650 Access Points • Brocade Mobility 6511 Access Point all – Upgrades firmware on all Brocade Mobility 6511 Access Points • Brocade Mobility 1220 Access Point all – Upgrades firmware on all Brocade Mobility 1220 Access Points • Brocade Mobility 71XX Access Point all – Upgrades firmware on all Brocade Mobility 71XX Access Points • Brocade Mobility 1240 Access Point all – Upgrades firmware on all Brocade Mobility 1240 Access Points • Brocade Mobility RFS4000 all – Upgrades firmware on all Brocade Mobility RFS4000s • Brocade Mobility RFS6000 all – Upgrades firmware on all Brocade Mobility RFS6000s • Brocade Mobility RFS7000 all – Upgrades firmware on all Brocade Mobility RFS7000s After selecting the device type, schedule an automatic upgrade and/or an automatic reboot.
no-reboot	Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)
reboot-time <TIME>	Optional. Schedules an automatic reboot after a successful upgrade • <TIME> – Optional. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.
upgrade-time <TIME> {no-reboot| reboot-time <TIME>}	Optional. Schedules an automatic firmware upgrade on all devices of the specified type • <TIME> – Specify the upgrade time in the MM/DD/YYYY-HH:MM or HH:MM format. The following actions can be performed after a scheduled upgrade: • no-reboot – Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted) • reboot-time <TIME> – Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.
staggered-reboot	This keyword is common to all of the above. • Optional. Enables staggered reboot (one at a time), without network impact

`device-upgrade cancel-upgrade [<MAC/HOSTNAME>|all]`

cancel-upgrade [<MAC/HOSTNAME>| all]	Cancels a scheduled firmware upgrade on a specified device or on all devices • <MAC/HOSTNAME> – Cancels a scheduled upgrade on the device identified by the <MAC/HOSTNAME> keyword. Specify the device's MAC address or hostname. • all – Cancels scheduled upgrade on all devices

	`device-upgrade cancel-upgrade [br650|br1220| br71xx|br81xx|rfs4000|rfs6000|rfs7000] all`
cancel-upgrade [br6511|br1220|br71xx| br81xx|rfs4000| rfs6000|rfs7000] all	Cancels scheduled firmware upgrade on all devices of a specific type. Select the device type. • Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point • Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000 • Service Platforms — Brocade Mobility RFS9510 • all – Cancels scheduled upgrade on all • Brocade Mobility 650 Access Point all – Cancels scheduled upgrade on all Brocade Mobility 650 Access Points • Brocade Mobility 6511 Access Point all – Cancels scheduled upgrade on all Brocade Mobility 6511 Access Points • Brocade Mobility 1220 Access Point all – Cancels scheduled upgrade on all Brocade Mobility 1220 Access Points • Brocade Mobility 71XX Access Point all – Cancels scheduled upgrade on all Brocade Mobility 71XX Access Points • Brocade Mobility 1240 Access Point all – Cancels scheduled upgrade on all Brocade Mobility 1240 Access Points • Brocade Mobility RFS4000 all – Cancels scheduled upgrade on all Brocade Mobility RFS4000s • Brocade Mobility RFS6000 all – Cancels scheduled upgrade on all Brocade Mobility RFS6000s • Brocade Mobility RFS7000 all – Cancels scheduled upgrade on all Brocade Mobility RFS7000s

	`device-upgrade cancel-upgrade on rf-domain [<DOMAIN-NAME>|all]`
cancel-upgrade on rf-domain [<RF-DOMAIN-NAME>| all]	Cancels scheduled firmware upgrade in a specified RF Domain or all RF Domains • <RF-DOMAIN-NAME> – Cancels scheduled device upgrade in a specified RF Domain. Specify the RF Domain name. • all – Cancels scheduled device upgrades across all RF Domains

```
device-upgrade load-image [br650|br6511|br1220|
br71xx|br81xx|rfs4000|rfs6000|rfs7000] <IMAGE-URL>
```

load-image [br6511|br71xx|br81xx|rfs 4000| rfs6000|rfs7000|]	Loads device firmware image from a specified location. Select the device type and provide the location of the required device firmware image. • Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point • Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000 • Service Platforms — Brocade Mobility RFS9510 • <IMAGE-URL> – Loads • firmware image • Brocade Mobility 650 Access Point <IMAGE-URL> – Loads Brocade Mobility 650 Access Point firmware image • Brocade Mobility 6511 Access Point <IMAGE-URL> – Loads Brocade Mobility 6511 Access Point firmware image • Brocade Mobility 1220 Access Point <IMAGE-URL> – Loads Brocade Mobility 1220 Access Point firmware image • Brocade Mobility 71XX Access Point <IMAGE-URL> – Loads Brocade Mobility 71XX Access Point firmware image • Brocade Mobility 1240 Access Point <IMAGE-URL> – Loads Brocade Mobility 1240 Access Point firmware image • Brocade Mobility RFS4000 <IMAGE-URL> – Loads Brocade Mobility RFS4000 firmware image • Brocade Mobility RFS6000 <IMAGE-URL> – Loads Brocade Mobility RFS6000 firmware image • Brocade Mobility RFS7000 <IMAGE-URL> – Loads Brocade Mobility RFS7000 firmware image
<IMAGE-URL>	Specify the device's firmware image location in one of the following formats: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>:<passwd>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb<n>:/path/file

```
device-upgrade rf-domain [<RF-DOMAIN-NAME>|all] [all|br650|br6511|
br1220|br71xx|br81xx|rfs4000|rfs6000|rfs7000]
{<MAC/HOSTNAME>|no-reboot|reboot-time <TIME>} {(staggered-reboot)}
```

rf-domain [<RF-DOMAIN-NAME>| all]	Upgrades firmware on devices in a specified RF Domain or all RF Domains. Devices within a RF Domain are upgraded through the RF Domain manager. • <RF-DOMAIN-NAME> – Upgrades devices in a specified RF Domain. Specify the RF Domain name. • all – Upgrades devices across all RF Domains
[all|br650|br6511|br1220 |br71xx|br81xx|rfs4000| rfs6000|rfs7000]	After specifying the RF Domain, select the device type. • all – Upgrades firmware on all devices Loads device firmware image from a specified location. Select the device type and provide the location of the required device firmware image. • Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point • Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000 • Service Platforms — Brocade Mobility RFS9510 • Brocade Mobility 650 Access Point – Upgrades firmware on all Brocade Mobility 650 Access Points • Brocade Mobility 6511 Access Point – Upgrades firmware on all Brocade Mobility 6511 Access Points • Brocade Mobility 1220 Access Point – Upgrades firmware on all Brocade Mobility 1220 Access Points • Brocade Mobility 71XX Access Point – Upgrades firmware on all Brocade Mobility 71XX Access Points • Brocade Mobility 1240 Access Point – Upgrades firmware on all Brocade Mobility 1240 Access Points • Brocade Mobility RFS4000 – Upgrades firmware on all Brocade Mobility RFS4000s • Brocade Mobility RFS6000 – Upgrades firmware on all Brocade Mobility RFS6000s • Brocade Mobility RFS7000 – Upgrades firmware on all Brocade Mobility RFS7000s
<MAC/HOSTNAME>	Optional. Upgrades firmware on the device identified by the <MAC/HOSTNAME> keyword • <MAC/HOSTNAME> – Specify the device's MAC address or hostname.
no-reboot {staggered-reboot}	Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)
reboot-time <TIME> {staggered-reboot}	Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.
staggered-reboot	This keyword is common to all of the above. • Optional. Enables staggered reboot (one at a time), without network impact

```
device-upgrade rf-domain [<RF-DOMAIN-NAME>|all] [all|br650|br6511|
br1220|br71xx|br81xx|rfs4000|rfs6000|rfs7000] {from-controller
{no-reboot|reboot-time <TIME>|upgrade-time <TIME> {no-reboot|
reboot-time <TIME>}} {(staggered-reboot)}
```

rf-domain [<RF-DOMAIN-NAME>| all]	Upgrades firmware on devices in a specified RF Domain or all RF Domains • <RF-DOMAIN-NAME> – Upgrades devices in a specified RF Domain. Specify the RF Domain name. • all – Upgrades devices across all RF Domains
[all|br650|br6511|br1220|br71xx|br81xx|rfs4000|rfs6000|rfs7000]	After specifying the RF Domain, select the device type. • all – Upgrades firmware on all devices Loads device firmware image from a specified location. Select the device type and provide the location of the required device firmware image. • Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point • Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000 • Service Platforms — Brocade Mobility RFS9510 • Brocade Mobility 650 Access Point – Upgrades firmware on all Brocade Mobility 650 Access Points • Brocade Mobility 6511 Access Point – Upgrades firmware on all Brocade Mobility 6511 Access Points • Brocade Mobility 1220 Access Point – Upgrades firmware on all Brocade Mobility 1220 Access Points • Brocade Mobility 71XX Access Point – Upgrades firmware on all Brocade Mobility 71XX Access Points • Brocade Mobility 1240 Access Point – Upgrades firmware on all Brocade Mobility 1240 Access Points • Brocade Mobility RFS4000 – Upgrades firmware on all Brocade Mobility RFS4000s • Brocade Mobility RFS6000 – Upgrades firmware on all Brocade Mobility RFS6000s • Brocade Mobility RFS7000 – Upgrades firmware on all Brocade Mobility RFS7000s
from-controller	Optional. Upgrades a device through the adopted device
no-reboot {staggered-reboot}	Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)
reboot-time <TIME> {staggered-reboot}	Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.
upgrade-time <TIME> {no-reboot| reboot-time <TIME>}	Optional. Schedules an automatic firmware upgrade • <TIME> – Specify the upgrade time in the MM/DD/YYYY-HH:MM or HH:MM format. After a scheduled upgrade, the following actions can be performed: • no-reboot – Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted) • reboot-time <TIME> – Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.
staggered-reboot	This keyword is common to all of the above. • Optional. Enables staggered reboot (one at a time), without network impact

```
device-upgrade rf-domain [<RF-DOMAIN-NAME>|all] [all|br650|br6511|
|br1220|br71xx|br81xx|rfs4000|rfs6000|rfs7000] {upgrade-time <TIME>
{no-reboot|reboot-time <TIME>}} {(staggered-reboot)}
```

rf-domain [<RF-DOMAIN-NAME>| all]	Upgrades firmware on devices in a specified RF Domain or all RF Domains • <RF-DOMAIN-NAME> – Upgrades devices in a specified RF Domain. Specify the RF Domain name. • all – Upgrades devices across all RF Domains
[all|br650|br6511|br1220|br71xx|br81xx|rfs4000|rfs6000|rfs7000]	After specifying the RF Domain, select the device type. • all – Upgrades firmware on all devices Loads device firmware image from a specified location. Select the device type and provide the location of the required device firmware image. • Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point • Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000 • Service Platforms — Brocade Mobility RFS9510 • Brocade Mobility 650 Access Point – Upgrades firmware on all Brocade Mobility 650 Access Points • Brocade Mobility 6511 Access Point – Upgrades firmware on all Brocade Mobility 6511 Access Points • Brocade Mobility 1220 Access Point – Upgrades firmware on all Brocade Mobility 1220 Access Points • Brocade Mobility 71XX Access Point – Upgrades firmware on all Brocade Mobility 71XX Access Points • Brocade Mobility 1240 Access Point – Upgrades firmware on all Brocade Mobility 1240 Access Points • Brocade Mobility RFS4000 – Upgrades firmware on all Brocade Mobility RFS4000s • Brocade Mobility RFS6000 – Upgrades firmware on all Brocade Mobility RFS6000s • Brocade Mobility RFS7000 – Upgrades firmware on all Brocade Mobility RFS7000s
upgrade <TIME>	Optional. Schedules an automatic device firmware upgrade • <TIME> – Specify the upgrade time in the MM/DD/YYYY-HH:MM or HH:MM format.
no-reboot {staggered-reboot}	Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)
reboot-time <TIME> {staggered-reboot}	Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.
staggered-reboot	This keyword is common to all of the above. • Optional. Enables staggered reboot (one at a time), without network impact

Usage Guidelines: (NOC controller adoption matrix)

The following table displays NOC controllers and the corresponding site-level controllers supported by each:

Site Controllers supported by each NOC controller	NOC Controllers
	Brocade Mobility RFS7000
Brocade Mobility RFS4000	X
Brocade Mobility RFS6000	X
Brocade Mobility RFS7000	X

Example

```
rfs4000-229D58>device-upgrade rfs4000-229D58 no-reboot
rfs4000-229D58>

rfs4000-229D58>show device-upgrade ?
  history            History of Device Upgrade
  load-image-status  Status of firmware file download on the device
```

```
  status             Status of Device Upgrade
  versions           Versions of device-upgrade images

rfs4000-229D58>show device-upgrade

rfs4000-229D58>show device-upgrade history
--------------------------------------------------------------------------------
--------------------
           Device      RESULT                TIME  RETRIES       UPGRADED-BY
LAST-UPDATE-ERROR
--------------------------------------------------------------------------------
--------------------

     br71xx-0F43D8     failed  2013-01-05 00:21:08       3  00-23-68-22-9D-58
Update error:  Unable to get update file, failure in ftp/openssl/tar

     ap6532-986C50     failed  2013-01-05 00:26:31       3  00-23-68-22-9D-58
Update error:  Bad file, failure in tar. tar: invalid tar magic
Total number of entries displayed: 2
rfs4000-229D58>

rfs4000-229D58>show device-upgrade versions
--------------------------------------------------------------------------------
---
          CONTROLLER              DEVICE-TYPE                  VERSION
--------------------------------------------------------------------------------
---
rfs4000-229D58              br650                 5.5.0.0-042B
rfs4000-229D58              br6511                none
rfs4000-229D58              br1220                5.5.0.0-042B
rfs4000-229D58              br71xx                none
rfs4000-229D58              br81xx                none
rfs4000-229D58              rfs4000               none
--------------------------------------------------------------------------------
---
rfs4000-229D58>
```

disable

User Exec Commands

This command can be executed in the Priv Exec Mode only. This command turns off (disables) the privileged mode command set and returns to the User Executable Mode. The prompt changes from `rfs7000-37FABE# to rfs7000-37FABE>`.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
disable
```

Parameters

None

Example

```
rfs7000-37FABE#disable
rfs7000-37FABE>
```

enable

User Exec Commands

Turns on (enables) the privileged mode command set. This command does not do anything in the Privilege Executable mode.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
enable
```

Parameters

None

Example

```
rfs7000-37FABE>enable
rfs7000-37FABE#
```

join-cluster

User Exec Commands

Adds a device (access point, wireless controller, or service platform), as a member, to an existing cluster of devices. Assign a static IP address to the device before adding to a cluster.

Supported in the following platforms:

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
join-cluster <IP> user <USERNAME> password <WORD> {level|mode}
join-cluster <IP> user <USERNAME> password <WORD> {level [1|2]|mode
[active|standby]}
```

Parameters

```
join-cluster <IP> user <USERNAME> password <WORD> {level [1|2]|mode
[active|standby]}
```

join-cluster	Adds a access point, wireless controller, or service platform to an existing cluster
<IP>	Specify the cluster member's IP address.
user <USERNAME>	Specify a user account with super user privileges on the new cluster member
password <WORD>	Specify password for the account specified in the user parameter
level [1|2]	Optional. Configures the routing level • 1 – Configures level 1 routing • 2 – Configures level 2 routing
mode [active|standby]	Optional. Configures the cluster mode • active – Configures this cluster as active • standby – Configures this cluster to be on standby mode

Usage Guidelines:

To add a device to an existing cluster:

- Configure a static IP address on the device (access point, wireless controller, or service platform).
- Provide username and password for superuser, network admin, system admin, or operator accounts.

After adding the device to a cluster, execute the "write memory" command to ensure the configuration persists across reboots.

Example

```
rfs7000-37FABE#join-cluster 172.16.10.10 user admin password admin123
Joining cluster at 172.16.10.10... Done
Please execute "write memory" to save cluster configuration.

rfs7000-37FABE#

nx6500-31FABE#join-cluster 172.16.10.10 user admin password admin123
Joining cluster at 172.16.10.10... Done
Please execute "write memory" to save cluster configuration.

nx6500-31FABE#
```

Related Commands:

cluster	Initiates cluster context. The cluster context enables centralized management and configuration of all cluster members from any one member.
create-cluster	Creates a new cluster on a specified device

l2tpv3

User Exec Commands

Establishes or brings down an *Layer 2 Tunnel Protocol Version 3* (L2TPV3) tunnel

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
l2tpv3 tunnel [<TUNNEL-NAME>|all]
l2tpv3 tunnel <TUNNEL-NAME> [down|session|up]
l2tpv3 tunnel <TUNNEL-NAME> [down|up] {on <DEVICE-NAME>}
l2tpv3 tunnel <TUNNEL-NAME> session <SESSION-NAME> [down|up] {on
<DEVICE-NAME>}

l2tpv3 tunnel all [down|up] {on <DEVICE-NAME>}
```

Parameters

`l2tpv3 tunnel <TUNNEL-NAME> [down|up] {on <DEVICE-NAME>}`

l2tpv3 tunnel	Establishes or brings down L2TPv3 tunnels
<TUNNEL-NAME> [down|up]	Specifies the tunnel name to establish or bring down • down – Brings down the specified tunnel • up – Establishes the specified tunnel
on <DEVICE-NAME>	Optional. Establishes or brings down a tunnel on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`l2tpv3 tunnel <TUNNEL-NAME> session <SESSION-NAME> [down|up] {on <DEVICE-NAME>}`

l2tpv3 tunnel	Establishes or brings down L2TPv3 tunnels
<TUNNEL-NAME> [session <SESSION-NAME>] [down|up]	Establishes or brings down a specified session inside an L2TPv3 tunnel • <TUNNEL-NAME> – Specify the tunnel name. • session <SESSION-NAME> – Specify the session name. • down – Brings down the specified session • up – Establishes the specified session
on <DEVICE-NAME>	Optional. Establishes or brings down a tunnel session on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`l2tpv3 tunnel all [down|up] {on <DEVICE-NAME>}`

l2tpv3 tunnel	Establishes or brings down L2TPv3 tunnels
all [down|up]	Establishes or brings down all L2TPv3 tunnels • down – Brings down all tunnels • up – Establishes all tunnels
on <DEVICE-NAME>	Optional. Establishes or brings down all tunnels on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Example

```
rfs7000-37FABE>l2tpv3 tunnel Tunnel1 session Tunnel1Session1 up on
rfs7000-37FABE
```

NOTE
For more information on the L2TPv3 tunnel configuration mode and commands, see *Chapter 23, L2TPV3-POLICY*.

logging

User Exec Commands

Modifies message logging settings

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
logging monitor
{<0-7>|alerts|critical|debugging|emergencies|errors|informational|
          notifications|warnings}
```

Parameters

```
logging monitor
{<0-7>|alerts|critical|debugging|emergencies|errors|informational|
notifications|warnings}
```

monitor	Sets the terminal lines logging levels. The logging severity levels can be set from 0 - 7. The system configures default settings, if no logging severity level is specified. • <0-7> – Optional. Specify the logging severity level from 0-7. The various levels and their implications are as follows: • alerts – Optional. Immediate action needed (severity=1) • critical – Optional. Critical conditions (severity=2) • debugging – Optional. Debugging messages (severity=7) • emergencies – Optional. System is unusable (severity=0) • errors – Optional. Error conditions (severity=3) • informational – Optional. Informational messages (severity=6) • notifications – Optional. Normal but significant conditions (severity=5) • warnings – Optional. Warning conditions (severity=4)

Example

```
rfs4000-229D58>logging monitor warnings

rfs4000-229D58>show logging

Logging module: enabled
    Aggregation time: disabled
    Console logging: level warnings
    Monitor logging: disabled
    Buffered logging: level warnings
    Syslog logging: level warnings
        Facility: local7
```

```
Log Buffer (522 bytes):

Apr 30 12:24:12 2013: rfs4000-229D58 : %SYSTEM-3-LOGIN_FAIL: Log-in failed for
user 'superuser' from 'pts/1'
Apr 30 12:24:12 2013: %AUTH-4-WARNING: login[2901]: login failed for
'superuser' on 'pts/1'
Apr 30 12:24:01 2013: rfs4000-229D58 : %SYSTEM-3-LOGIN_FAIL: Log-in failed for
user 'exit' from 'pts/1'
Apr 30 12:24:01 2013: %AUTH-4-WARNING: login[2901]: login failed for 'exit' on
'pts/1'
Apr 29 14:50:28 2013: rfs4000-229D58 : %SYSTEM-3-UI_USER_AUTH_FAIL: UI user
'Admin' from: '192.168.100.207' authentication failed
rfs4000-229D58>
```

Related Commands:

no	Resets terminal lines logging levels

mint

User Exec Commands

Uses MiNT protocol to perform a ping and traceroute to a remote device

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
mint [ping|traceroute]

mint ping <MINT-ID> {(count <1-10000>|size <1-64000>|timeout <1-10>)}

mint traceroute <MINT-ID> {(destination-port <1-65535>|max-hops <1-255>|
          source-port <1-65535>|timeout <1-255>)}
```

Parameters

```
mint ping <MINT-ID> {(count <1-10000>|size <1-64000>|timeout <1-10>)}
```

ping <MINT-ID>	Sends a MiNT echo message to a specified destination • <MINT-ID> – Specify the destination device's MiNT ID.
count <1-10000>	Optional. Sets the pings to the MiNT destination • <1-60> – Specify a value from 1 - 10000. The default is 3.
size <1-64000>	Optional. Sets the MiNT payload size in bytes • <1-64000> – Specify a value from 1 - 640000 bytes. The default is 64 bytes.
timeout <1-10>	Optional. Sets a response time in seconds • <1-10> – Specify a value from 1 sec - 10 sec. The default is 1 second.

```
mint traceroute <MINT-ID> {(destination-port <1-65535>|max-hops <1-255>|
source-port <1-65535>|timseout <1-255>)}
```

traceroute <MINT-ID>	Prints the route packets trace to a device • <MINT-ID> – Specify the destination device's MiNT ID.
destination-port <1-65535>	Optional. Sets the *Equal-cost Multi-path* (ECMP) routing destination port • <1-65535> – Specify a value from 1 - 65535. The default port is 45.
max-hops <1-255>	Optional. Sets the maximum number of hops a traceroute packet traverses in the forward direction • <1-255> – Specify a value from 1 - 255. The default is 30.
source-port <1-65535>	Optional. Sets the ECMP source port • <1-65535> – Specify a value from 1 - 65535. The default port is 45.
timeout <1-255>	Optional. Sets the minimum response time period in seconds • <1-65535> – Specify a value from 1 sec - 255 sec. The default is 30 seconds.

Example

```
rfs7000-37FABE>mint ping 70.37.FA.BF count 20 size 128
MiNT ping 70.37.FA.BF with 128 bytes of data.
 Response from 70.37.FA.BF: id=1 time=0.292 ms
 Response from 70.37.FA.BF: id=2 time=0.206 ms
 Response from 70.37.FA.BF: id=3 time=0.184 ms
 Response from 70.37.FA.BF: id=4 time=0.160 ms
 Response from 70.37.FA.BF: id=5 time=0.138 ms
 Response from 70.37.FA.BF: id=6 time=0.161 ms
 Response from 70.37.FA.BF: id=7 time=0.174 ms
 Response from 70.37.FA.BF: id=8 time=0.207 ms
 Response from 70.37.FA.BF: id=9 time=0.157 ms
 Response from 70.37.FA.BF: id=10 time=0.153 ms
 Response from 70.37.FA.BF: id=11 time=0.159 ms
 Response from 70.37.FA.BF: id=12 time=0.173 ms
 Response from 70.37.FA.BF: id=13 time=0.156 ms
 Response from 70.37.FA.BF: id=14 time=0.209 ms
 Response from 70.37.FA.BF: id=15 time=0.147 ms
 Response from 70.37.FA.BF: id=16 time=0.203 ms
 Response from 70.37.FA.BF: id=17 time=0.148 ms
 Response from 70.37.FA.BF: id=18 time=0.169 ms
 Response from 70.37.FA.BF: id=19 time=0.164 ms
 Response from 70.37.FA.BF: id=20 time=0.177 ms

--- 70.37.FA.BF ping statistics ---
20 packets transmitted, 20 packets received, 0% packet loss
round-trip min/avg/max = 0.138/0.177/0.292 ms
rfs7000-37FABE>
```

no

User Exec Commands

Use the no command to revert a command or to set parameters to their default. This command turns off an enabled feature or reverts settings to default.

NOTE
The commands have their own set of parameters that can be reset.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no
[adoption|captive-portal|crypto|debug|logging|mac-user-db|page|service|termin
al|
          virtual-machine|wireless]

no adoption {on <DEVICE-OR-DOMAIN-NAME>}

no captive-portal client [captive-portal <CAPTIVE-PORTAL-NAME>|mac <MAC>]
          {on <DEVICE-OR-DOMAIN-NAME>}

no crypto pki [server|trustpoint]
no crypto pki [server|trustpoint] <TRUSTPOINT-NAME> {del-key {on
<DEVICE-NAME>}|
          on <DEVICE-NAME>}

no logging monitor

no mac-user-db user [<USER-NAME>|all]

no page

no service [enable|locator]
no service enable [l2tpv3|radiusd]
no service locator {on <DEVICE-NAME>}

no terminal [length|width]

no virtual-machine assign-usb-ports {on <DEVICE-NAME>}

no wireless client [all|<MAC>]
no wireless client all {filter|on}
no wireless client all {filter [wlan <WLAN-NAME>]}
no wireless client all {on <DEVICE-OR-DOMAIN-NAME>} {filter [wlan
<WLAN-NAME>]}
no wireless client mac <MAC> {on <DEVICE-OR-DOMAIN-NAME>}
```

Parameters

```
no adoption {on <DEVICE-OR-DOMAIN-NAME>}
```

no adoption {on <DEVICE-OR-DOMAIN-NAME>}	Resets the adoption status of a specified device or all devices • <DEVICE-OR-DOMAIN-NAME> – Optional. Specify the name of the AP, wireless controller, service platform, or RF Domain. If an RF Domain is specified, the system resets status of all adopted devices within the specified domain.

`no captive-portal client [captive-portal <CAPTIVE-PORTAL-NAME>|mac <MAC>] {on <DEVICE-OR-DOMAIN-NAME>}`

no captive-portal client	Disconnects captive portal clients from the network
captive-portal <CAPTIVE-PORTAL-NAME>	Disconnects clients of the captive portal identified by the <CAPTIVE-PORTAL-NAME> keyword • <CAPTIVE-PORTAL-NAME> – Specify the captive portal name.
mac <MAC>	Disconnects a client specified by its MAC address • <MAC> – Specify the client's MAC address.
on <DEVICE-OR-DOMAIN-NAME>	Optional. Disconnects clients on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

`no crypto pki [server|trustpoint] <TRUSTPOINT-NAME> {del-key {on <DEVICE-NAME>}| on <DEVICE-NAME>}`

no crypto pki	Deletes all PKI authentications
[server|trustpoint] <TRUSTPOINT-NAME>	Deletes PKI authentications, such as server certificates and trustpoints • server – Deletes server certificates • trustpoint – Deletes a trustpoint and its associated certificates The following keyword is common to the 'server' and 'trustpoint' parameters: • <TURSTPOINT-NAME> – Deletes a trustpoint or its server certificate. Specify the trustpoint name.
del-key {on <DEVICE-NAME>}	Optional. Deletes the private key associated with a server certificate or trustpoint. The operation fails if the private key is in use by other trustpoints. • on <DEVICE-NAME> – Optional. Deletes the private key on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`no logging monitor`

no logging monitor	Resets terminal lines message logging levels

`no mac-user-db user [<USER-NAME>|all]`

no mac-user-db user	Deletes a specified user or all users from the MAC registration user database This command is available only on the NX9000 series service platforms.
<USER-NAME>	Deletes the user, identified by the <USER-NAME> keyword, from the MAC registration user database • <USER-NAME> – Specify the username.
all	Deletes all users from the MAC registration user database

`no page`

no page	Resets paging to its default. Disabling paging displays the CLI command output at once, instead of page by page.

`no service enable [l2tpv3|radiusd]`

no service	Disables specified services or features
enable [l2tpv3|radiusd]	Disables the following features: • l2tpv3 – Disables L2TPV3 • radiusd – Disables loading of the RADIUS server on low memory devices

	`no service locator {on <DEVICE-NAME>}`
no service	Disables LEDs on a specified device or all devices in the WLAN. It also resets the CLI table expand and MiNT protocol configurations.
locator {on <DEVICE-NAME>}	Disables LEDs on a specified device • on <DEVICE-NAME> – Optional. Specify the name of the AP, wireless controller, or service platform. If no device name is specified, the system disables LEDs on all devices in the WLAN.

	`no terminal [length|width]`
no terminal [length|width]	Resets the width of the terminal window or the number of lines displayed within the terminal window • length – Resets the number of lines displayed on the terminal window to its default • width – Resets the width of the terminal window to its default

	`no virtual-machine assign-usb-ports {on <DEVICE-NAME>}`
no virtual-machine assign-usb-ports	Reverts ports assigned for virtual-machines back to Mobility This command is available only on the Brocade Mobility RFS9510 series service platforms.
on <DEVICE-NAME>	Reverts virtual-machine assigned ports on a specified device • on <DEVICE-NAME> – Optional. Specify the name of the AP, wireless controller, or service platform.

	`no wireless client all {filter [wlan <WLAN-NAME>]}`
no wireless client all	Disassociates all clients on a specified device or domain
filter [wlan <WLAN-NAME>]	Optional. Specifies additional client selection filter • wlan – Filters clients on a specified WLAN • <WLAN-NAME> – Specify the WLAN name.

	`no wireless client all {on <DEVICE-OR-DOMAIN-NAME>} {filter [wlan <WLAN-NAME>]}`
no wireless client all {on <DEVICE-OR-DOMAIN-NAME>}	Disassociates all wireless clients on a specified device or domain • on <DEVICE-OR-DOMAIN-NAME> – Optional. Specify the name of the AP, wireless controller, service platform, or RF Domain.
filter [wlan <WLAN-NAME>]	The following are optional filter parameters: • filter – Optional. Specifies additional client selection filter • wlan – Filters clients on a specified WLAN • <WLAN-NAME> – Specify the WLAN name.

	`no wireless client mac <MAC> {on <DEVICE-OR-DOMAIN-NAME>}`
no wireless client mac <MAC>	Disassociates a single wireless client on a specified device or RF Domain • mac <MAC> – Specify the wireless client's MAC address in the AA-BB-CC-DD-EE-FF format.
on <DEVICE-OR-DOMAIN-NAME>	Optional. Specifies the name of the AP, wireless controller, service platform, or RF Domain to which the specified client is associated

Usage Guidelines:

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
rfs7000-37FABE>no adoption

rfs7000-37FABE>no page

rfs7000-37FABE>no service cli-tables-expand line
```

Related Commands:

auto-provisioning-policy	Resets the adoption state of a device and all devices adopted to it
captive portal	Manages captive portal clients
crypto	Enables digital certificate configuration and RSA Keypair management.
logging	Modifies message logging settings
page	Resets paging to its default
service	Performs different functions depending on the parameter passed
terminal	Sets the length or the number of lines displayed within the terminal window
virtual-machine	Installs, configures, and monitors the status of third-party *virtual machines* (VMs). This command is specific to the Brocade Mobility RFS9510 series service platforms.
wireless-client	Manages wireless clients

page

User Exec Commands

Toggles a device's paging function. Enabling this command displays the CLI command output page by page, instead of running the entire output at once.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
page
```

Parameters

None

Example

```
rfs7000-37FABE>page
rfs7000-37FABE>
```

Related Commands:

no	Disables device paging

ping

User Exec Commands

Sends *Internet Controller Message Protocol* (ICMP) echo messages to a user-specified location

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
ping <IP/HOSTNAME> {count <1-10000>|dont-fragment {count|size}|size <1-64000>}
```

Parameters

```
ping <IP/HOSTNAME> {count <1-10000>|dont-fragment {count|size}|size <1-64000>}
```

<IP/HOSTNAME>	Specify the destination IP address or hostname. When entered without any parameters, this command prompts for an IP address or a hostname.
count <1-10000>	Optional. Sets the pings to the specified destination • <1-10000> – Specify a value from 1 - 10000. The default is 5.
dont-fragment {count|size}	Optional. Sets the don't fragment bit in the ping packet. Packets with the dont-fragment bit specified are not fragmented. When a packet, with the dont-fragment bit specified, exceeds the specified *maximum transmission unit* (MTU) value, an error message is sent from the device trying to fragment it. • count <1-10000> – Optional. Sets the pings to the specified destination from 1 - 10000. The default is 5. • size – <1-64000> – Optional. Sets the size of ping payload size from 1 - 64000 bytes. The default is 100 bytes.
size <1-64000>	Optional. Sets the ping payload size in bytes • <1-64000> – Specify the ping payload size from 1 - 64000. The default is 100 bytes.

Example

```
rfs7000-37FABE>ping 172.16.10.4 count 6
PING 172.16.10.4 (172.16.10.4): 100 data bytes
108 bytes from 172.16.10.4: seq=0 ttl=64 time=0.851 ms
108 bytes from 172.16.10.4: seq=1 ttl=64 time=0.430 ms
108 bytes from 172.16.10.4: seq=2 ttl=64 time=0.509 ms
108 bytes from 172.16.10.4: seq=3 ttl=64 time=0.507 ms
108 bytes from 172.16.10.4: seq=4 ttl=64 time=0.407 ms
108 bytes from 172.16.10.4: seq=5 ttl=64 time=0.402 ms

--- 172.16.10.4 ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 0.402/0.517/0.851 ms
rfs7000-37FABE>
```

ssh

User Exec Commands

Opens a *Secure Shell* (SSH) connection between two network devices

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
ssh <IP/HOSTNAME> <USER-NAME>
```

Parameters

```
ssh <IP/HOSTNAME> <USER-NAME>
```

[<IP/HOSTNAME>]	Specify the IP address or hostname of the remote system.
<USERNAME>	Specify the name of the user requesting SSH connection with the remote system.

Example

```
rfs7000-37FABE>ssh 172.16.10.4 admin
The authenticity of host '172.16.10.4 (172.16.10.4)' can't be established.
RSA key fingerprint is 82:b7:27:86:de:08:e8:53:9f:d6:a3:88:aa:1f:e8:ff.
Are you sure you want to continue connecting (yes/no)?
```

telnet

User Exec Commands

Opens a Telnet session between two network devices

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
telnet <IP/HOSTNAME> {<TCP-PORT>}
```

Parameters

```
telnet <IP/HOSTNAME> {<TCP-PORT>}
```

<IP/HOSTNAME>	Configures the destination remote system's IP address or hostname. The Telnet session is established between the connecting system and the remote system. • <IP/HOSTNAME> – Specify the remote system's IP address or hostname.
<TCP-PORT>	Optional. Specify the *Transmission Control Protocol* (TCP) port number.

Example

```
rfs4000-229D58>telnet 192.168.13.9

Entering character mode
Escape character is '^]'.
```

```
Brocade Mobility RFS4000 release 5.5.0.0-018D
rfs4000-229D58 login:
```

terminal

User Exec Commands

Sets the length or the number of lines displayed within the terminal window

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
terminal [length|width] <0-512>
```

Parameters

```
terminal [length|width] <0-512>
```

length <0-512>	Sets the number of lines displayed on a terminal window • <0-512> – Specify a value from 0 - 512.
width <0-512>	Sets the width (the number of characters displayed) of the terminal window • <0-512> – Specify a value from 0 - 512.

Example

```
rfs7000-37FABE>terminal length 150

rfs7000-37FABE>terminal width 215

rfs7000-37FABE>show terminal
Terminal Type: xterm
Length: 150     Width: 215
rfs7000-37FABE>
```

Related Commands:

no	Resets the width and length of the terminal window

time-it

User Exec Commands

Verifies the time taken by a particular command between request and response

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
time-it <COMMAND>
```

Parameters

```
time-it <COMMAND>
```

time-it <COMMAND>	Verifies the time taken by a particular command to execute and provide a result • <COMMAND> – Specify the command.

Example

```
rfs7000-37FABE>time-it enable
That took 0.00 seconds..
rfs7000-37FABE#
```

traceroute

User Exec Commands

Traces the route to a defined destination

Use '--help' or '-h' to display a complete list of parameters for the traceroute command

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
traceroute <LINE>
```

Parameters

```
traceroute <LINE>
```

traceroute <LINE>	Traces the route to a destination IP address or hostname • <LINE> – Specify a traceroute argument. For example, "service traceroute-h".

Example

```
rfs7000-37FABE>traceroute --help
BusyBox v1.14.1 () multi-call binary

Usage: traceroute [-FIldnrv] [-f 1st_ttl] [-m max_ttl] [-p port#] [-q
nqueries]
        [-s src_addr] [-t tos] [-w wait] [-g gateway] [-i iface]
        [-z pausemsecs] HOST [data size]
Trace the route to HOST
```

```
Options:
        -F      Set the don't fragment bit
        -I      Use ICMP ECHO instead of UDP datagrams
        -l      Display the ttl value of the returned packet
        -d      Set SO_DEBUG options to socket
        -n      Print hop addresses numerically rather than symbolically
        -r      Bypass the normal routing tables and send directly to a host
        -v      Verbose
        -m max_ttl      Max time-to-live (max number of hops)
        -p port#        Base UDP port number used in probes (default is 33434)
        -q nqueries     Number of probes per 'ttl' (default 3)
        -s src_addr     IP address to use as the source address
        -t tos          Type-of-service in probe packets (default 0)
        -w wait         Time in seconds to wait for a response (default 3 sec)
        -g              Loose source route gateway (8 max)

rfs7000-37FABE>

rfs7000-37FABE>traceroute 172.16.10.1
traceroute to 172.16.10.1 (172.16.10.1), 30 hops max, 38 byte packets
 1  172.16.10.1 (172.16.10.1)  0.423 ms  0.145 ms  0.225 ms
rfs7000-37FABE>
```

watch

User Exec Commands

Repeats the specified CLI command at periodic intervals

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
watch <1-3600> <LINE>
```

Parameters

```
watch <1-3600> <LINE>
```

watch	Repeats a CLI command at a specified interval (in seconds)
<1-3600>	Select an interval from 1 - 3600 sec. Pressing CTRL-Z halts execution of the command.
<LINE>	Specify the CLI command.

Example

```
rfs7000-37FABE>watch 45 page

rfs7000-37FABE>watch 45 ping 172.16.10.2
PING 172.16.10.2 (172.16.10.2): 100 data bytes
108 bytes from 172.16.10.2: seq=0 ttl=64 time=0.725 ms
108 bytes from 172.16.10.2: seq=1 ttl=64 time=0.464 ms
```

```
108 bytes from 172.16.10.2: seq=2 ttl=64 time=0.458 ms
108 bytes from 172.16.10.2: seq=3 ttl=64 time=0.378 ms
108 bytes from 172.16.10.2: seq=4 ttl=64 time=0.364 ms

--- 172.16.10.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.364/0.477/0.725 ms
rfs7000-37FABE>
```

exit

User Exec Commands

Ends the current CLI session and closes the session window

For more information, see *exit*.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
exit
```

Parameters

None

Example

```
rfs7000-37FABE>exit
```

virtual-machine

User Exec Commands

Installs, configures, and monitors the status of third-party *virtual machines* (VMs)

In addition to the Brocade shipped VMs and Brocade Mobility RFS9510 series service platforms support the installation and administration of third-party VMs. However, the third-party VMs supported by these devices varies.

The third-party VMs supported on Brocade Mobility RFS9510 are:

- ADSP
- TEAM-CMT

Use the virtual-machine command to install the third-party VMs, and configure parameters, such as install media type and location, number of *Virtual Central Processing Units* (VCPUS), VM memory, VM disk, number of *Virtual Network Interfaces* (VIFs), and *Virtual Networking Computing* (VNC) port.

Installing third-party VMs saves on hardware cost and provides a unified VM management interface.

- Syntax Brocade Mobility RFS9510

Supported in the following platforms:

- Service Platforms — Brocade Mobility RFS9510

`virtual-machine assign-usb-ports team-vowlan {on <DEVICE-NAME>}`

assign-usb-ports team-vowlan	Assigns USB ports to TEAM-VoWLAN on a specified device • on <DEVICE-NAME> – Optional. Specify the device name. Use the `no > virtual-machine > assign-usb-ports` to reassign the port to Mobility. TEAM-RLS VM cannot be installed when USB ports are assigned to TEAM-VoWLAN.

`virtual-machine console [<VM-NAME>|team-urc|team-rls|team-vowlan]`

virtual-machine console	Connects to the VM's console, based on the parameters passed. Select one of the following console options: • <VM-NAME> – Connects to the console of the VM identified by the <VM-NAME> keyword. Specify the VM name. • team-urc – Connects to the VM TEAM Unified Retail Communication's (URC) (IP-PBX) console • team-rls – Connects to the VM TEAM *Radio Link Service* (RLS) server's console • team-vowlan – Connects to the VM TEAM-VoWLAN's (Voice over WLAN) console

`virtual-machine export <VM-NAME> [<FILE>|<URL>] {on <DEVICE-NAME>}`

virtual-machine export	Exports an existing VM image and settings. Use this command to export the VM to another NX45XX or device in the same domain. • <VM-NAME> – Specify the VM name. • <FILE> – Specify the location and name of the source file (VM image). The VM image is retrieved and exported from the specified location. • <URL> – Specify the destination location. This is the location to which the VM image is copied. Use one of the following formats to provide the destination path: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>:<passwd>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file • on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices • <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas. The VM should be in a stop state during the export process. If the destination is a device, the image is copied to a predefined location (VM archive)

	`virtual-machine install <VM-NAME> type [disk|iso disk-size <SIZE>|vm-archive] install-media [<FILE>|<URL>|<USB>] {autostart|memory|on|vcpus|vif-count|vnc}`
virtual-machine install	Installs the VM. The install command internally creates a VM template, consisting of the specified parameters, and starts the installation process. • <VM-NAME> – Specify the VM name. • type – Specify the install-media (image) type. The options are: • disk – Specifies the install media type as pre-installed OS disk image (located in the flash memory) • iso disk-size <SIZE> – Specifies the install media type as ISO file. This is a single file, which contains the OS bootable install media. • disk-size <SIZE> – If the install media type is ISO, specify the disk size in GB. • vm-archive – Specifies the install media type as VM archive. The VM archive file is a tar.gz file consisting of a pre-installed OS disk image and an associated configuration file. The configuration is a standard libvirt VM template consisting of VM specific information. After specifying the install media type, specify the location of the image. The image can be located in any of the following supported locations: FLASH, USB, or a remote location, such as http, ftp, sftp, tftp.
install-media [<FILE>|<URL>|<USB>]	Specifies the install media location • <FILE> – Specifies the install-media file is located on flash, for example flash:/cache • <URL> – Specifies the install-media file is located on a remote URL. Provide the URL using one of the following formats: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>:<passwd>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file • <USB> – Specifies the install-media file is located on a USB. Provide the USB path and file name using the following format: usb<n>:/path/file After specifying the image location, you may provide the following information: • autostart – Optional. Specifies whether to autostart the VM on system reboot • ignore – Enables autostart on each system boot/reboot • start – Disables autostart (default setting) • memory – Optional. Defines the VM memory size • <512-8192> – Specify the VM memory from 512 - 8192 MB. The default is 2048 MB. • on – Optional. Executes the command on a specified device • <DEVICE-NAME> – Specify the service platform name. • vcpus – Optional. Specifies the number of VCPUS for this VM • <1-4> – Specify the number of VCPUS from 1- 4. The default setting is 4. Contd...
	• vif-count – Optional. Configures or resets the VIF number for this VM • <0-2> – Specify the VIF number from 0 - 2. the default setting is 1. If assigning a virtual network interface for the VM, optionally specify the following parameters: • vif-mac – Sets the MAC index for the virtual interfaces 1 & 2. • vif-to-vmif – Maps the virtual interface (1 or 2) to the selected VMIF interface. Specify the VMIF interface index from 1 - 8. VMIFs are layer 2 interfaces on the Mobility bridge. Each custom VM can have up to a maximum of 2 virtual Ethernet interfaces. By default, these interfaces are internally connected to the Dataplane bridge through VMIF1, which is an untagged port with access VLAN 1. • vnc – Enables or disables VNC on the virtual interfaces 1 & 2 • vnc – Optional. Disables/enables VNC port. When enabled, provides remote access to VGA through the noVNC client. • disable – Disables VNC • enable – Enables VNC (default setting)

	`virtual-machine install [team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}`
virtual-machine install	Installs the VM. The install command internally creates a VM template, consisting of the specified parameters, and starts the installation process. Select one of the following options: • team-urc – Installs the VM TEAM-URC image • team-rls – Installs the VM TEAM-RLS image • team-vowlan – Installs the VM TEAM-VoWLAN image The following keywords are common to all of the above parameters: • on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices • <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas.

	`virtual-machine restart [<VM-NAME>|hard|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}`
virtual-machine restart	Restarts the VM • <VM-NAME> – Restarts the VM identified by the <VM-NAME> keyword • team-urc – Restarts the VM TEAM-URC • team-rls – Restarts the VM TEAM-RLS • team-vowlan – Restarts the VM TEAM-VoWLAN The following keywords are common to all of the above parameters: • on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices • <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas. The option '*hard*' forces the specified VM to restart.

```
virtual-machine set [autostart [ignore|start]|memory <512-8192>|vcpus <1-4>|
vif-count <0-2>|vif-mac <VIF-INDEX> <MAC-INDEX>|vif-to-vmif <VIF-INDEX>
<VMIF-INDEX>|
vnc [disable|enable]] [<VM-NAME>|team-urc|team-rls|team-vowlan] {on
<DEVICE-NAME>}
```

virtual-machine set	Configures the VM settings
	• autostart – Specifies whether to autostart the VM on system reboot
	  • ignore – Enables autostart on each system reboot
	  • start – Disables autostart
	• memory – Defines the VM memory size
	  • <512-8192> – Specify the VM memory from 512 - 8192 MB. The default is 1024 MB.
	• vcpus – Specifies the number of VCPUS for this VM
	  • <1-4> – Specify the number of VCPUS from 1- 4.
	• vif-count – Configures or resets the VM's VIFs
	  • <0-2> – Specify the VIF number from 0 - 2.
	• vif-mac – Configures the MAC address of the selected virtual network interface
	  • <1-2> – Select the VIF
	  • <1-8> – Specify the MAC index for the selected VIF
	  • <MAC> – Specify the customized MAC address for the selected VIF in the AA-BB-CC-DD-EE-FF format.
	Each VM has a maximum of two network interfaces (indexed 1 and 2, referred to as VIF). By default, each VIF is automatically assigned a MAC from the range allocated for that device. However, you can use the 'set' keyword to specify the MAC from within the allocated range. Each of these VIFs are mapped to a layer 2 port in the dataplane (referred to as VMIF). These VMIFs are standard l2 ports on the DP bridge, supporting all VLAN and ACL commands. Mobility 5.5 supports up to a maximum of 8 VMIFs. By default, a VM's interface is always mapped to VMIF1. You can map a VIF to any of the 8 VMIFs. Use the vif-to-vmif command to map a VIF to a VMIF on the DP bridge.
	• vif-to-vmif – Maps the virtual interface (1 or 2) to the selected VMIF interface. Specify the VMIF interface index from 1 - 8.
	Mobility provides a dataplane bridge for external network connectivity for VMs. VM Interfaces define which IP address is associated with each VLAN ID the service platform is connected to and enables remote service platform administration. Each custom VM can have up to a maximum of two VM interfaces.
	By default, VM interfaces are internally connected to the dataplane bridge via VMIF1. VMIF1, by default, is an untagged port providing access to VLAN 1 to support the capability to connect the VM interfaces to any of the VMIF ports. This provides the flexibility to move a VM interface onto different VLANs as well as configure specific firewall and QOS rules.
	• vnc – Disables/enables VNC port option for an existing VM. When enabled, provides remote access to VGA through the noVNC client.
	  • disable – Disables VNC port
	  • enable – Enables VNC port
	Contd...

	After configuring the VM settings, identify the VM to apply the settings. • <VM-NAME> – Applies these settings to the VM identified by the <VM-NAME> keyword. Specify the VM name. • team-urc – Applies these settings to the VM TEAM-URC • team-rls – Applies these settings to the VM TEAM-RLS • team-vowlan – Applies these settings to the VM TEAM-VoWLAN

	`virtual-machine start [<VM-NAME>|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}`
virtual-machine start	Starts the VM, based on the parameters passed. Select one of the following options: • <VM-NAME> – Starts the VM identified by the <VM-NAME> keyword. Specify the VM name. • team-urc – Starts the VM TEAM-URC • team-rls – Starts the VM TEAM-RLS • team-vowlan – Starts the VM TEAM-VoWLAN The following keywords are common to all of the above parameters: • on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices • <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas.
	`virtual-machine stop [<VM-NAME>|hard|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}`
virtual-machine stop	Stops the VM, based on the parameters passed. Select one of the following options: • <VM-NAME> – Stops the VM identified by the <VM-NAME> keyword. Specify the VM name. • team-urc – Stops the VM TEAM-URC • team-rls – Stops the VM TEAM-RLS • team-vowlan – Stops the VM TEAM-VoWLAN The following keywords are common to all of the above parameters: • on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices • <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas. The option 'hard' forces the selected VM to shutdown.
	`virtual-machine uninstall [<VM-NAME>|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}`
virtual-machine uninstall	Uninstalls the specified VM • <VM-NAME> – Uninstalls the VM identified by the <VM-NAME> keyword. Specify the VM name. • team-urc – Uninstalls the VM TEAM-URC • team-rls – Uninstalls the VM TEAM-RLS • team-vowlan – Uninstalls the VM TEAM-VoWLAN The following keywords are common to all of the above parameters: • on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices • <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas. This command releases the VM's resources, such as memory, VCPUS, VNC port, disk space, and removes the RF Domain reference from the system.

Syntax: Brocade Mobility RFS9510

```
virtual-machine
virtual-machine console [<VM-NAME>|adsp|team-cmt]
virtual-machine install [adsp|team-cmt] {on <DEVICE-NAME>}
virtual-machine restart [adsp|team-cmt] {on <DEVICE-NAME>}
virtual-machine set disk-size <100-500> adsp {on <DEVICE-NAME>}
virtual-machine set memory <512-8192> [adsp|team-cmt] {on <DEVICE-NAME>}
virtual-machine set Mobility-memory <12288-32739>
virtual-machine [start|stop] [adsp|team-cmt] {on <DEVICE-NAME>}
virtual-machine uninstall [adsp|team-cmt] {on <DEVICE-NAME>}
```

ParametersBrocade Mobility RFS9510

	`virtual-machine console [adsp|team-cmt]`
virtual-machine console	Connects to the ADSP or TEAM-CMT VM's console, based on the parameters passed. Select one of the following console options: • <VM-NAME> – Connects to the console of the VM identified by the <VM-NAME> keyword. Specify the VM name. • adsp – Connects to the *Air-Defense Services Platform* (ADSP) VM's management console • team-cmt – Connects to TEAM-CMT VM's management console When ADSP is running on the Brocade Mobility RFS9510 model service platforms, Mobility communicates with ADSP using a *single sign-on* (SSO) authentication mechanism. Once the user is logged in, Mobility gains access to ADSP without being prompted to login again at ADSP. However, the Mobility and ADSP databases are not synchronized. ADSP has its own user database, stored locally within its VM, which is accessed whenever a user logs directly into ADSP. Mobility and ADSP must be consistent in the manner events are reported up through a network hierarchy to ensure optimal interoperability and event reporting. To provide such consistency, Mobility has added support for an ADSP-like hierarchal tree. The tree resides within Mobility, and ADSP reads it from Mobility and displays the network hierarchy in its own ADSP interface. The hierarchal tree can also be used to launch ADSP modules (like Spectrum Analyzer) directly from Mobility. For more information on configuring Mobility tree-node structure, see *tree-node*.

	`virtual-machine install [adsp|team-cmt] {on <DEVICE-NAME>}`

virtual-machine install	Installs the ADSP or TEAM-CMT VM, based on the parameter passed
	• on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices
	• <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas.
	Before installing the ADSP VM, execute the upgrade command, giving the path and file name of the ADSP firmware image. This extracts the image on to the device (Brocade Mobility RFS9510) on which the command has been executed. On successful completion of this process, execute the reload command to reboot the device. Once the device has been successfully rebooted, execute the *virtual-machine > install > adsp* command.
	For example:
	`nx9500-6C874D#upgrade tftp://20.1.1.60/adsp-9.1.1Aug 20 15:12:41 2013: %DAEMON-6-INFO: lighttpd[2405]: 127.0.0.1 127.0.0.1:443 - "POST /mapi.fcgi HTTP/1.1" 200 192 "-" "-"`
	`-03-5.5.0.0-072B.img`
	`Aug 20 15:12:51 2013: nx9500-6C874D : %DIAG-6-NEW_LED_STATE: LED state message FIRMWARE_UPGRADE_STARTED from module led_msg`
	`Running from partition /dev/sda8`
	`Validating image file header`
	`Extracting files (this may take some time).....Aug 20 15:12:53 2013: %DAEMON-6-INFO: lighttpd[2405]: 127.0.0.1 127.0.0.1:443 - "POST /mapi.fcgi HTTP/1.1" 200 923 "-" "-".....`

	`virtual-machine restart [adsp|team-cmt] {on <DEVICE-NAME>}`
virtual-machine restart	Restarts the ADSP or TEAM-CMT VM, based on the parameter passed • on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices • <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas.

	`virtual-machine set disk-size <100-500> adsp {on <DEVICE-NAME>}`
virtual-machine set disk-size	Sets the ADSP VM's disk size (in GB). Specify a value from 100 - 500 GB. • on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices • <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas. Stop the ADSP VM before executing this command.

	`virtual-machine set memory <512-8192> [adsp|team-cmt] {on <DEVICE-NAME>}`
virtual-machine set memory	Modifies the ADSP or TEAM-CMT VM's memory, in MB, based on the parameter passed. Specify a value from 512 - 8192 MB. • on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices • <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas.
	`virtual-machine set Mobility-memory <12288-32739>`
virtual-machine set Mobility-memory <12288-32739>	Specifies the Mobility memory size in MB This command is applicable only to the Brocade Mobility RFS9510 service platforms. Use the *show > virtual-machine-configuration* command to view the configured memory allocation. Use the *show > virtual-machine-statistics* to view the current allocated memory allocation. • <12288-32739> – Specify a value from 12288 - 32739 MB. The default is 18432 MB. The new memory setting takes effect only after the next boot.
	`virtual-machine [start|stop] [adsp|team-cmt] {on <DEVICE-NAME>}`
virtual-machine [start|stop]	Starts/stops the ADSP or TEAM-CMT VM, based on the parameter passed • start – Starts the ADSP or TEAM-CMT VM. Use this command to boot a shut down VM (in a stop state). • stop – Stops a running ADSP or TEAM-CMT VM. Use this command to shut down a running VM. • on <DEVICE-NAME> – Optional. Executes the start/stop command on a specified device or devices • <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas.
	`virtual-machine uninstall [adsp|team-cmt] {on <DEVICE-NAME>}`
virtual-machine uninstall	Uninstalls the ADSP or TEAM-CMT VM based on the parameter passed • on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices • <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas.

Example

```
The following examples show the VM installation process:

Insatllation media: USB

<DEVICE>#virtual-machine install <VM-NAME> type iso disk-size 8 install-media
usb1://vms/win7.iso autostart start memory 512 vcpus 3 vif-count 2 vnc enable

Installation media: pre-installed disk image

<DEVICE>#virtual-machine install <VM-NAME> type disk install-media
flash:/vms/win7_disk.img autostart start memory 512 vcpus 3 vif-count 2
vnc-enable  on <DEVICE-NAME>

In the preceding example, the command is executed on the device identified by
the <DEVICE-NAME> keyword. In such a scenario, the disk-size is ignored if
specified. The VM has the install media as first boot device.

Installation media: VM archive

<DEVICE>#virtual-machine install type vm-archive install-media
flash:/vms/<VM-NAME> vcpus 3

In the preceding example, the default configuration attached with the VM
archive overrides any parameters specified.
```

```
Exporting an installed VM:

<DEVICE>#virtual-machine export <VM-NAME> <URL> on <DEVICE-NAME>

In the preceding example, the command copies the VM archive on to the URL (VM
should be in stop state).

nx4500-5CFA2B>virtual-machine install team-urc
Virtual Machine install team-urc command successfully sent.
nx4500-5CFA2B>
```

NOTE
Use the show > virtual-machine > [configuration|debugging|export|statistics] command to view installed VM details.

Chapter

PRIVILEGED EXEC MODE COMMANDS 3

Most PRIV EXEC commands set operating parameters. Privileged-level access should be password protected to prevent unauthorized use. The PRIV EXEC command set includes commands contained within the USER EXEC mode. The PRIV EXEC mode also provides access to configuration modes, and includes advanced testing commands.

The PRIV EXEC mode prompt consists of the hostname of the device followed by a pound sign (#).

To access the PRIV EXEC mode, enter the following at the prompt:

```
<DEVICE>>enable
<DEVICE>#
```

The PRIV EXEC mode is often referred to as the enable mode, because the enable command is used to enter the mode.

There is no provision to configure a password to get direct access to PRIV EXEC (enable) mode.

```
<DEVICE>#?
Privileged command commands:
  archive                      Manage archive files
  boot                         Boot commands
  captive-portal-page-upload   Captive portal advanced page upload
  cd                           Change current directory
  change-passwd                Change password
  clear                        Clear
  clock                        Configure software system clock
  cluster                      Cluster commands
  commit                       Commit all changes made in this session
  configure                    Enter configuration mode
  connect                      Open a console connection to a remote device
  copy                         Copy from one file to another
  create-cluster               Create a cluster
  crypto                       Encryption related commands
  debug                        Debugging functions
  delete                       Deletes specified file from the system.
  device-upgrade               Device firmware upgrade
  diff                         Display differences between two files
  dir                          List files on a filesystem
  disable                      Turn off privileged mode command
  edit                         Edit a text file
  enable                       Turn on privileged mode command
  erase                        Erase a filesystem
  halt                         Halt the system
  help                         Description of the interactive help system
  join-cluster                 Join the cluster
  l2tpv3                       L2tpv3 protocol
  logging                      Modify message logging facilities
  mint                         MiNT protocol
  mkdir                        Create a directory
  more                         Display the contents of a file
  no                           Negate a command or set its defaults
  page                         Toggle paging
```

```
  ping                      Send ICMP echo messages
  pwd                       Display current directory
  raid                      RAID operations
  re-elect                  Perform re-election
  reload                    Halt and perform a warm reboot
  remote-debug              Troubleshoot remote system(s)
  rename                    Rename a file
  revert                    Revert changes
  rmdir                     Delete a directory
  self                      Config context of the device currently logged
                            into
  service                   Service Commands
  show                      Show running system information
  smart-cache               Content Cache Operation
  ssh                       Open an ssh connection
  telnet                    Open a telnet connection
  terminal                  Set terminal line parameters
  time-it                   Check how long a particular command took between
                            request and completion of response
  traceroute                Trace route to destination
  upgrade                   Upgrade software image
  upgrade-abort             Abort an ongoing upgrade
  virtual-machine           Virtual Machine
  watch                     Repeat the specific CLI command at a periodic
                            interval
  write                     Write running configuration to memory or
                            terminal

  clrscr                    Clears the display screen
  exit                      Exit from the CLI

<DEVICE>#
```

Privileged Exec Mode Commands

Table 1 summarizes the PRIV EXEC Mode commands.

TABLE 1 Privileged Exec Commands

Command	Description	Reference
archive	Manages file archive operations	page 78
boot	Specifies the image used after rebooti	page 80
captive-portal-page-upload	Uploads captive portal advanced pages	page 81
cd	Changes the current directory	page 83
change-passwd	Changes the password of a logged user	page 83
clear	Clears parameters, cache entries, table entries, and other similar entries	page 84
clock	Configures the system clock	page 93
cluster	Initiates a cluster context	page 93
configure	Enters the configuration mode	page 94
connect	Begins a console connection to a remote device	page 95

TABLE 1 Privileged Exec Commands (Continued)

Command	Description	Reference
copy	Copies a file from any location to the wireless controller, service platform, or access point	page 95
create-cluster	Creates a new cluster on a specified device	page 96
crypto	Enables encryption	page 97
delete	Deletes a specified file from the system	page 107
device-upgrade	Configures device firmware upgrade parameters	page 108
diff	Displays the differences between two files	page 115
dir	Displays the list of files on a file system	*page 3-116*
disable	Disables the privileged mode command set	*page 3-117*
edit	Edits a text file	page 118
enable	Turns on (enables) the privileged mode commands set	page 119
erase	Erases a file system	page 119
halt	Halts a device (access point, wireless controller, or service platform)	page 120
join-cluster	Adds a device (access point, wireless controller, or service platform), as cluster member, to an existing cluster of devices	*page 3-121*
l2tpv3	Establishes or brings down *Layer 2 Tunneling Protocol Version* 3 (L2TPV3) tunnels	*page 3-122*
logging	Modifies message logging parameters	page 123
mint	Configures MiNT protocols	page 124
mkdir	Creates a new directory in the file system	page 126
more	Displays the contents of a file	page 127
no	Reverts a command or sets values to their default	page 127
page	Toggles a device's (access point, wireless controller, or service platform) paging function	page 131
ping	Sends ICMP echo messages to a user-specified location	page 132
pwd	Displays the current directory	page 133
re-elect	Re-elects the tunnel controller (wireless controller, service platform, or access point)	page 134
reload	Halts a device (wireless controller, service platform, or access point) and performs a warm reboot	page 134
rename	Renames a file in the existing file system	page 135
rmdir	Deletes an existing file from the file system	page 137
self	Displays the configuration context of the device	page 138
ssh	Connects to another device using a secure shell	page 138
telnet	Opens a Telnet session	page 139
terminal	Sets the length and width of the terminal window	page 140
time-it	Verifies the time taken by a particular command between request and response	page 140
traceroute	Traces the route to a defined destination	page 141
upgrade	Upgrades the software image	page 141
upgrade-abort	Aborts an ongoing software image upgrade	page 142
watch	Repeats a specified CLI command at a periodic interval	page 143

TABLE 1 Privileged Exec Commands (Continued)

Command	Description	Reference
virtual-machine	Installs, configures, and monitors the status of *virtual machines* (VMs). This command is specific to the Brocade Mobility RFS9510 series service platforms.	page 144
clrscr	Clears the display screen	page 385
commit	Commits (saves) the changes made in the current session	page 386
help	Displays interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug (config-if) instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425
exit	Ends the current CLI session and closes the session window	*page 3-144*

archive

Privileged Exec Mode Commands

Manages file archive operations

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
archive tar /table [<FILE>|<URL>]
archive tar /create [<FILE>|<URL>] <FILE>
archive tar /xtract [<FILE>|<URL>] <DIR>
```

Parameters

```
archive tar /table [<FILE>|<URL>]
```

tar	Manipulates (creates, lists, or extracts) a tar file
/table	Lists the files in a tar file
<FILE>	Defines a tar filename
<URL>	Sets the tar file URL

```
archive tar /create [<FILE>|<URL>] <FILE>
```

tar	Manipulates (creates, lists or extracts) a tar file
/create	Creates a tar file
<FILE>	Defines tar filename
<URL>	Sets the tar file URL

```
archive tar /xtract [<FILE>|<URL>] <DIR>
```

tar	Manipulates (creates, lists or extracts) a tar file
/xtract	Extracts content from a tar file
<FILE>	Defines tar filename
<URL>	Sets the tar file URL
<DIR>	Specify a directory name. When used with /create, dir is the source directory for the tar file. When used with /xtract, dir is the destination file where contents of the tar file are extracted.

Example

Following examples show how to zip the folder flash:/log/?

```
rfs4000-229D58#dir flash:/
Directory of flash:/

  drwx             Wed Jan 30 02:45:10 2013   log
  drwx             Sat Jan  1 00:00:09 2000   configs
  drwx             Sat Jan  1 00:00:08 2000   cache
  drwx             Wed Jan 16 22:26:53 2013   crashinfo
  drwx             Wed Jan  2 22:23:41 2013   testdir
  drwx             Wed Jan 16 22:57:14 2013   archived_logs
  drwx             Sat Jan  1 00:00:08 2000   upgrade
  drwx             Sat Jan  1 00:00:09 2000   hotspot
  drwx             Sat Jan  1 00:00:09 2000   floorplans
  drwx             Sat Jan  1 00:00:09 2000   startuplog

rfs4000-229D58#

rfs4000-229D58#archive tar /create flash:/out.tar flash:/log
log/
log/cfgd.log
log/cfgd.log.1
log/vlan-usage.log
log/anald.log
log/anald.startup
log/dpd2.log
log/dpd2.startup
log/upgrade.log
log/messages.log
log/startup.log
log/hotplug/
log/hotplug/events
log/radius/
rfs4000-229D58#

rfs4000-229D58#dir flash:/
Directory of flash:/

  drwx             Wed Jan 30 02:45:10 2013   log
  drwx             Sat Jan  1 00:00:09 2000   configs
  drwx             Sat Jan  1 00:00:08 2000   cache
  drwx             Wed Jan 16 22:26:53 2013   crashinfo
  drwx             Wed Jan  2 22:23:41 2013   testdir
  drwx             Wed Jan 16 22:57:14 2013   archived_logs
  drwx             Sat Jan  1 00:00:08 2000   upgrade
  drwx             Sat Jan  1 00:00:09 2000   hotspot
  drwx             Sat Jan  1 00:00:09 2000   floorplans
```

```
  drwx             Sat Jan  1 00:00:09 2000   startuplog
  -rw-   176128    Fri Feb 15 14:32:51 2013   out.tar

rfs4000-229D58#
```

boot

Privileged Exec Mode Commands

Specifies the image used after reboot

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
boot system [primary|secondary] {on <DEVICE-NAME>}
```

Parameters

```
boot system [primary|secondary] {on <DEVICE-NAME>}
```

system [primary|secondary]	Specifies the image used after a device reboot • primary – Uses the primary image after reboot • secondary – Uses the secondary image after reboot
on <DEVICE-NAME>	Optional. Specifies the primary or secondary image location on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Example

```
rfs4000-229D58#show boot
------------------------------------------------------------------------------
---
     IMAGE            BUILD DATE             INSTALL DATE          VERSION
------------------------------------------------------------------------------
---
  Primary       01:29:2013 22:34:21     01:16:2013 22:34:00     5.5.0.0-018D
  Secondary     01:25:2013 21:56:47     01:13:2013 22:57:12     5.5.0.0-017D
------------------------------------------------------------------------------
---
Current Boot       : Primary
Next Boot          : Primary
Software Fallback  : Enabled
rfs4000-229D58#

rfs4000-229D58#boot system secondary
Updated system boot partition
rfs4000-229D58#

rfs4000-229D58#show boot
------------------------------------------------------------------------------
---
```

```
     IMAGE            BUILD DATE             INSTALL DATE          VERSION
-------------------------------------------------------------------------------
---
  Primary       01:29:2013 22:34:21     01:16:2013 22:34:00     5.5.0.0-018D
  Secondary     01:25:2013 21:56:47     01:13:2013 22:57:12     5.5.0.0-017D
-------------------------------------------------------------------------------
---
Current Boot       : Primary
Next Boot          : Secondary
Software Fallback  : Enabled
rfs4000-229D58#
```

captive-portal-page-upload

Privileged Exec Mode Commands

Uploads captive portal advanced pages

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
captive-portal-page-upload [<CAPTIVE-PORTAL-NAME>|cancel-upload|load-file]

captive-portal-page-upload <CAPTIVE-PORTAL-NAME>
[<MAC/HOSTNAME>|all|rf-domain]

captive-portal-page-upload <CAPTIVE-PORTAL-NAME> [<MAC/HOSTNAME>|all]
          {upload-time <TIME>}

captive-portal-page-upload <CAPTIVE-PORTAL-NAME> rf-domain
[<DOMAIN-NAME>|all]
          {from-controller} {(upload-time <TIME>)}

captive-portal-page-upload cancel-upload [<MAC/HOSTNAME>|all|on rf-domain
[<DOMAIN-
          NAME>|all]]

captive-portal-page-upload load-file <CAPTIVE-PORTAL-NAME> <URL>
```

Parameters

```
captive-portal-page-upload <CAPTIVE-PORTAL-NAME> [<MAC/HOSTNAME>|all]
{upload-time <TIME>}
```

captive-portal-page-upload <CAPTIVE-PORTAL-NAME>	Uploads advanced pages specified by the <CAPTIVE-PORTAL-NAME> parameter • <CAPTIVE-PORTAL-NAME> – Specify captive portal name (should be existing and configured).
<MAC/HOSTNAME>	Uploads to a specified AP • <MAC/HOSTNAME> – Specify the AP's MAC address or hostname.

all	Uploads to all APs
upload-time <TIME>	Optional. Schedules an upload time • <TIME> – Specify upload time in the MM/DD/YYYY-HH:MM or HH:MM format.
	`captive-portal-page-upload <CAPTIVE-PORTAL-NAME> rf-domain [<DOMAIN-NAME>|all] {from-controller} {(upload-time <TIME>)}`
captive-portal-page-upload <CAPTIVE-PORTAL-NAME>	Uploads advanced pages specified by the <CAPTIVE-PORTAL-NAME> parameter • <CAPTIVE-PORTAL-NAME> – Specify captive portal name (should be existing and configured).
rf-domain [<DOMAIN-NAME>|all]	Uploads to all APs within a specified RF Domain or all RF Domains • <DOMAIN-NAME> – Uploads to APs within a specified RF Domain. Specify the RF Domain name. • all – Uploads to APs across all RF Domains
from-controller	Optional. Uploads to APs from the adopted device
upload-time <TIME>	Optional. Schedules an AP upload • <TIME> – Specify upload time in the MM/DD/YYYY-HH:MM or HH:MM format.
	`captive-portal-page-upload cancel-upload [<MAC/HOSTNAME>|all|on rf-domain [<DOMAIN-NAME>|all]]`
captive-portal-page-upload cancel-upload	Cancels a scheduled AP upload
cancel-upload [<MAC/HOSTNAME>| all| on rf-domain [<DOMAIN-NAME>| all]]	Select one of the following options: • <MAC/HOSTNAME> – Cancels a scheduled upload to a specified AP. Specify the AP MAC address or hostname. • all – Cancels all scheduled AP uploads • on rf- domain – Cancels all scheduled uploads within a specified RF Domain or all RF Domains • <DOMAIN-NAME> – Cancels scheduled uploads within a specified RF Domain. Specify RF Domain name. • all – Cancels scheduled uploads across all RF Domains
	`captive-portal-page-upload load-file <CAPTIVE-PORTAL-NAME> <URL>`
captive-portal-page-upload load-file	Loads captive-portal advanced pages
<CAPTIVE-PORTAL-NAME> <URL>	Specify captive portal name (should be existing and configured) and location. • <URL> – Specifies file location in one of the following format: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>:<passwd>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb<n>:/path/file

Example

```
rfs4000-229D58>captive-portal-page-upload test1 00-04-96-4A-A7-08 upload-time
03/01/2013-12:30
------------------------------------------------------------------------------
---
        CONTROLLER          STATUS                      MESSAGE
------------------------------------------------------------------------------
---
  00-23-68-22-9D-58       Fail       Failed to initiate page upload
```

```
-------------------------------------------------------------------------------
---
rfs4000-229D58>

rfs4000-229D58>captive-portal-page-upload cancel-upload 00-04-96-4A-A7-08
-------------------------------------------------------------------------------
---
         CONTROLLER             STATUS                    MESSAGE
-------------------------------------------------------------------------------
---
  00-23-68-22-9D-58         Success         Cancelled upgrade of 1 APs
-------------------------------------------------------------------------------
---
rfs4000-229D58>
```

cd

Privileged Exec Mode Commands

Changes the current directory

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
cd {<DIR>}
```

Parameters

```
cd {<DIR>}
```

<DIR>	Optional. Changes the current directory to <DIR>. If a directory name is not provided, the system displays the current directory.

Example

```
rfs7000-37FABE#cd flash:/log/
rfs7000-37FABE#pwd
flash:/log/
rfs7000-37FABE#
```

change-passwd

Privileged Exec Mode Commands

Changes the password of a logged user. When this command is executed without any parameters, the password can be changed interactively.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
change-passwd {<OLD-PASSWORD>} <NEW-PASSWORD>
```

Parameters

```
change-passwd {<OLD-PASSWORD>} <NEW-PASSWORD>
```

<OLD-PASSWORD>	Optional. Specify the password to be changed.
<NEW-PASSWORD>	Specify the new password. **NOTE:** The password can also be changed interactively. To do so, press [**Enter**] after the command.

Usage Guidelines:

A password must be from 1 - 64 characters.

Example

```
rfs7000-37FABE#change-passwd
Enter old password:
Enter new password:
Password for user 'admin' changed successfully
Please write this password change to memory(write memory) to be persistent.
rfs7000-37FABE#write memory
OK
rfs7000-37FABE#
```

clear

Privileged Exec Mode Commands

Clears parameters, cache entries, table entries, and other entries. The clear command is available for specific commands only. The information cleared using this command varies depending on the mode where the clear command is executed.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

NOTE
Refer to the interface details below when using `clear`
- ge <index> – Brocade Mobility RFS4000 supports 5 GEs, Brocade Mobility RFS6000 supports 8 GEs, Brocade Mobility RFS7000 supports 4 GEs
- me1 – Available in both Brocade Mobility RFS7000 and Brocade Mobility RFS6000
- up1– Uplink interface on Brocade Mobility RFS4000

Syntax:

```
clear
[arp-cache|cdp|counters|crypto|event-history|firewall|gre|ip|l2tpv3-stats|

license|lldp|logging|mac-address-table|mint|role|rtls|smart-cache|spanning-tr
ee|
          vrrp]

clear arp-cache {on <DEVICE-NAME>}

clear [cdp|lldp] neighbors {on <DEVICE-NAME>}

clear counters [all|br|bridge|interface|radio|router|thread|wireless-client]
clear counters [all|bridge|router|thread]
clear counters [br|wireless-client] {<MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}
clear counters interface [<INTERFACE-NAME>|all|ge <1-5>|me1|port-channel
<1-3>|pppoe1|
          vlan <1-4094>|wwan1]
clear counters radio {<MAC/HOSTNAME>|on}
clear counters radio {<MAC/HOSTNAME> <1-3>} {(on <DEVICE-OR-DOMAIN-NAME>)}

clear crypto [ike|ipsec]
clear crypto ike sa [<IP>|all] {on <DEVICE-NAME>}
clear crypto ipsec sa {on <DEVICE-NAME>}

clear event-history

clear firewall [dhcp snoop-table|dos stats|flows] {on <DEVICE-NAME>}

clear gre stats {on <DEVICE-NAME>}

clear ip [dhcp|ospf]
clear ip dhcp bindings [<IP>|all] {on <DEVICE-NAME>}
clear ip ospf process {on <DEVICE-NAME>}

clear l2tpv3-stats tunnel <L2TPV3-TUNNEL-NAME> {on <DEVICE-NAME>|session
<SESSION-
          NAME> {on <DEVICE-NAME>}}

clear license [borrowed|lent]
clear license borrowed {on <DEVICE-NAME>}
clear license lent to <DEVICE-NAME> {on <DEVICE-NAME>}

clear logging {on <DEVICE-NAME>}

clear mac-address-table {address|interface|vlan} {on <DEVICE-NAME>}

clear mac-address-table {address <MAC>|vlan <1-4094>} {on <DEVICE-NAME>}
clear mac-address-table interface [<IF-NAME>|ge <1-X>|port-channel <1-X>|
          t1e1 <1-4> <1-1>|up <1-X>|vmif <1-X>|xge <1-4>] {on <DEVICE-NAME>}
```

```
clear mint mlcp history {on <DEVICE-NAME>}

clear role ldap-stats {on <DEVICE-NAME>}

clear rtls [aeroscout|ekahau]
clear rtls [aeroscout|ekahau] {<DEVICE-NAME> {on <DEVICE-OR-DOMAIN-NAME>}|
          on <DEVICE-OR-DOMAIN-NAME>}

clear spanning-tree detected-protocols {interface|on <DEVICE-NAME>}
clear spanning-tree detected-protocols {interface [<INTERFACE-NAME>|ge
<1-5>|me1|
          port-channel <1-3>|pppoe1|vlan <1-4094>|wwan1]} {on <DEVICE-NAME>}

clear vrrp [error-stats|stats] {on <DEVICE-NAME>}
```

Parameters

`clear arp-cache {on <DEVICE-NAME>}`

arp-cache	Clears *Address Resolution Protocol* (ARP) cache entries on a device
on <DEVICE-NAME>	Optional. Clears ARP cache entries on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`clear [cdp|lldp] neighbors {on <DEVICE-NAME>}`

cdp	Clears *Cisco Discovery Protocol* (CDP) table entries
ldp	Clears *Link Layer Discovery Protocol* (LLDP) neighbor table entries
neighbors	Clears CDP or LLDP neighbor table entries based on the option selected in the preceding step
on <DEVICE-NAME>	Optional. Clears CDP or LLDP neighbor table entries on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`clear counters [all|bridge|router|thread]`

counters [all|bridge|router|thread]	Clears counters on a system • all – Clears all counters irrespective of the interface type • bridge – Clears bridge counters • router – Clears router counters • thread – Clears per-thread counters

`clear counters [br|wireless-client] {<MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}`

counters [br|wireless-client]	Clears counters on a system • br – Clears access point wireless counters • wireless-client – Clears wireless client counters
<MAC>	The following keyword is common to the 'br' and 'wireless-client' parameters: • <MAC> – Optional. Clears counters of the AP/wireless client identified by the <MAC> keyword. Specify the MAC address of the AP or wireless client. The system clears all AP or wireless client counters, if no MAC address is specified.
on <DEVICE-OR-DOMAIN-NAME>	The following keyword is recursive and is applicable to the <MAC> parameter: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Clears AP/wireless-client counters on a specified device or RF Domain If no MAC address is specified, the system clears all AP or wireless client counters on the specified AP, wireless controller, service platform, or RF Domain.

`clear counters interface [<INTERFACE-NAME>|all|ge <1-5>|me1|port-channel <1-3>| pppoe1|vlan <1-4094>|wwan1]`

counters interface [<INTERFACE-NAME>|all| ge <1-5>|me1| port-channel <1-3>| pppoe1|vlan <1-4094>| wwan1]	Clears interface counters for a specified interface • <INTERFACE-NAME> – Clears a specified interface counters. Specify the interface name. • all – Clears all interface counters • ge <1-5> – Clears GigabitEthernet interface counters. Specify the GigabitEthernet interface index from 1 - 5. • me1 – Clears FastEthernet interface counters • port-channel <1- 3> – Clears port-channel interface counters. Specify the port channel interface index from 1 - 3. • pppoe1 – Clears *Point-to-Point Protocol over Ethernet* (PPPoE) interface counters • vlan <1-4094> – Clears interface counters. Specify the *Switch Virtual Interface* (SVI) VLAN ID from 1 - 4094. • wwan1 – Clears wireless WAN interface counters

`clear counters radio {<MAC/HOSTNAME> <1-3>} {(on <DEVICE-OR-DOMAIN-NAME>)}`

counters radio	Clears wireless radio counters
<MAC/HOSTNAME> <1-3>	Clears counters of a radio identified by the <MAC/HOSTNAME> keyword. • <MAC/HOSTNAME> – Optional. Specify the hostname or MAC address. Optionally, append the interface number to form radio ID in the form of AA-BB-CC-DD-EE-FF:RX or HOSTNAME:RX • <1-3> – Optional. Specify the radio index (if not specified as part of the radio ID). The system clears all radio counters, if no MAC address or radio index is specified.
on <DEVICE-OR-DOMAIN-NAME>	The following keyword is recursive and is applicable to the <MAC> parameter: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Clears AP/wireless-client counters on a specified device or RF Domain If no MAC address is specified, the system clears all AP or wireless client counters on the specified AP, wireless controller, service platform, or RF Domain.

`clear crypto ike sa [<IP>|all] {on <DEVICE-NAME>}`

crypto	Clears encryption module database
ike sa [<IP>|all]	Clears *Internet Key Exchange* (IKE) *security associations* (SAs) • <IP> – Clears IKE SAs for a certain peer • all – Clears IKE SAs for all peers
on <DEVICE-NAME>	Optional. Clears IKE SA entries, for a specified peer or all peers, on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`clear crypto ipsec sa {on <DEVICE-NAME>}`

crypto	Clears encryption module database
ipsec sa {on <DEVICE-NAME>}	Clears *Internet Protocol Security* (IPSec) database SAs • on <DEVICE-NAME> – Optional. Clears IPSec SA entries on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`clear event-history`

event-history	Clears event history cache entries

`clear firewall [dhcp snoop-table|dos stats|flows] {on <DEVICE-NAME>}`

firewall	Clears firewall event entries
DHCP snoop-table	Clears DHCP snoop table entries
dos stats	Clears denial of service statistics

flows	Clears established firewall sessions
on <DEVICE-NAME>	The following keywords are common to the DHCP, DOS, and flows parameters: • on <DEVICE-NAME> – Optional. Clears DHCP snoop table entries, denial of service statistics, or the established firewall sessions on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`clear gre stats {on <DEVICE-NAME>}`

gre stats	Clears GRE tunnel statistics
on <DEVICE-NAME>	Optional. GRE tunnel statistics on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`clear ip dhcp bindings [<IP>|all] {on <DEVICE-NAME>}`

ip	Clears a *Dynamic Host Configuration Protocol* (DHCP) server's IP address bindings entries
dhcp bindings	Clears DHCP server's connections and address binding entries
<IP>	Clears specific address binding entries. Specify the IP address to clear binding entries.
all	Clears all address binding entries
on <DEVICE-NAME>	Optional. Clears a specified address binding or all address bindings on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`clear ip ospf process {on <DEVICE-NAME>}`

ip ospf process	Clears already enabled *open shortest path first* (OSPF) process and restarts the process
on <DEVICE-NAME>	Optional. Clears OSPF process on a specified device OSPF is a link-state *interior gateway protocol* (IGP). OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighbor routers and constructs a network topology. The topology determines the routing table presented to the Internet layer which makes routing decisions based solely on the destination IP address found in IP packets. • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`clear l2tpv3-stats tunnel <L2TPV3-TUNNEL-NAME> {on <DEVICE-NAME>|session <SESSION-NAME> {on <DEVICE-NAME>}}`

l2tpv3-stats	Clears L2TPv3 tunnel session statistics
tunnel <L2TPV3-TUNNEL-NAME>	Clears all sessions associated with a specified L2TPv3 tunnel • <L2TPV3-TUNNEL-NAME> – Specify the L2TPv3 tunnel name.
{on <DEVICE-NAME>| session <SESSION-NAME> {on <DEVICE-NAME>}}	Use the following optional parameters to specify a session or device. • on <DEVICE-NAME> – Optional. Clears all sessions associated with the specified L2TPv3 tunnel running on a specified device • DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. • session <SESSION-NAME> – Optional. Clears a specified L2TPv3 tunnel session. Specify the session name. • on <DEVICE-NAME> – Optional. Specifies the device running the L2TPv3 tunnel session • DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. If no optional parameters are specified, the system clears all L2TPv3 tunnel session statistics.

`clear license borrowed {on <DEVICE-NAME>}`

license borrowed {on <DEVICE-NAME>}	Releases or revokes all licenses borrowed by a site controller • on <DEVICE-NAME> – Optional. Specifies the borrowing controller's name. If no device name is specified, the system clears all borrowed licenses on the logged device.

`clear license lent to <DEVICE-NAME> {on <DEVICE-NAME>}`

license lent	NOC controller releases or revokes all licenses loaned to a site controller
to <DEVICE-NAME>	Specifies the borrowing controller's name • <DEVICE-NAME> – Specify the controller's name.
on <DEVICE-NAME>	Optional. Specifies the controller's name If no device name is specified, the system clears all loaned licenses on the logged device.

`clear mac-address-table {address <MAC>|vlan <1-4094>} {on <DEVICE-NAME>}`

mac-address-table	Clears the MAC address forwarding table
address <MAC>	Optional. Clears a specified MAC address from the MAC address table. • <MAC> – Specify the MAC address in one of the following formats: AA-BB-CC-DD-EE-FF or AA:BB:CC;DD:EE:FF or AABB.CCDD.EEFF
vlan <1-4094>	Optional. Clears all MAC addresses for a specified VLAN • <1-4094> – Specify the VLAN ID from 1 - 4094
on <DEVICE-NAME>	Optional. Clears a single entry or all MAC entries for the specified VLAN in the MAC address forwarding table on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`clear mac-address-table interface [<IF-NAME>|ge <1-X>|port-channel <1-X>|t1e1 <1-4> <1-1>|up <1-2>|vmif <1-X>|xge <1-4>] {on <DEVICE-NAME>}`

mac-address-table	Clears the MAC address forwarding table
interface	Clears all MAC addresses for the selected interface. Use the options available to specify the interface.
<IF-NAME>	Clears MAC address forwarding table for the specified layer 2 interface (Ethernet port) • <IF-NAME> – Specify the layer 2 interface name.
ge <1-X>	Clears MAC address forwarding table for the specified GigabitEthernet interface • <1-X> – Specify the GigabitEthernet interface index from 1 - X. The number of Ethernet interfaces supported varies for different device types. Brocade Mobility RFS4000 supports 5 GE interfaces.
port-channel <1-X>	Clears MAC address forwarding table for the specified port-channel interface • <1-X> – Specify the port-channel interface index from 1 - X. The number of port-channel interfaces supported varies for different device types. Brocade Mobility RFS4000 supports 3 port-channels.
t1e1 <1-4> <1-1>	Clears MAC address forwarding table for the specified T1E1L interface • <1-4> – Specify the T1E1 interface index from 1 - 4. A maximum of 4 slots are available. Select the slot to clear the MAC address forwarding table.
up <1-X>	Clears MAC address forwarding table for the WAN Ethernet interface The number of WAN Ethernet interfaces supported varies for different devices. The Brocade Mobility RFS4000 and Brocade Mobility RFS6000 devices support 1 WAN Ethernet interface. The NX45XX supports 2 WAN Ethernet interfaces.
vmif <1-X>	Clears MAC address forwarding table for the VM interface • <1-X> – Specify the VM interface index from 1 - X. The VMIF interfaces are supported only on the Brocade Mobility RFS9510 series service platforms. The number of supported VMIFs varies for different device types.

xge <1-4>	Clears MAC address forwarding table for the specified TenGigabitEthernet interface • <1-4> – Specify the GigabitEthernet interface index from 1 - 4. This interface is supported only on the NX9000 series service platforms.
on <DEVICE-NAME>	Optional. Clears the MAC address forwarding table, for the selected interface, on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`clear mint mlcp history {on <DEVICE-NAME>}`

mint	Clears MiNT related information
mlcp history	Clears *MiNT Link Creation Protocol* (MLCP) client history
on <DEVICE-NAME>	Optional. Clears MLCP client history on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform

`clear role ldap-stats {on <DEVICE-NAME>}`

role ldap-stats	Clears role based LDAP server statistics
on <DEVICE-NAME>	Optional. Clears role based LDAP server statistics on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`clear rtls [aeroscout|ekahau] {<DEVICE-NAME> {on <DEVICE-OR-DOMAIN-NAME>}| on <DEVICE-OR-DOMAIN-NAME>}`

rtls	Clears *Real Time Location Service* (RTLS) statistics
aeroscout	Clears RTLS Aeroscout statistics
ekahau	Clears RTLS Ekahau statistics
<DEVICE-NAME>	This keyword is common to the ‘aeroscout’ and ‘ekahau’ parameters. • <DEVICE-NAME> – Optional. Clears Aeroscout or Ekahau RTLS statistics on a specified device
<DEVICE-OR-DOMAIN-NAME>	This keyword is common to the ‘aeroscout’ and ‘ekahau’ parameters. • <DEVICE-OR-DOMAIN-NAME> – Optional. Clears Aeroscout or Ekahau RTLS statistics on a specified device or RF Domain. Specify the name of the AP, wireless controller, service platform, or RF Domain.

`clear spanning-tree detected-protocols {on <DEVICE-NAME>}`

spanning-tree	Clears spanning tree protocols on an interface, and also restarts protocol migration
detected-protocols	Restarts protocol migration
on <DEVICE-NAME>	Optional. Clears spanning tree protocols on a specified device • <DEVICE-NAME> – Optional. Specify the name of the AP, wireless controller, or service platform.

`clear spanning-tree detected-protocols {interface [<INTERFACE-NAME>|ge <1-5>|me1| port-channel <1-3>|pppoe1|vlan <1-4094>|wwan1]} {on <DEVICE-NAME>}`

spanning-tree	Clears spanning tree protocols on an interface and restarts protocol migration
detected-protocols	Restarts protocol migration

interface [<INTERFACE-NAME>| ge <1-5>|me1| port-channel <1-3>| pppoe1|vlan <1-4094>| wwan1]	Optional. Clears spanning tree entries on different interfaces • <INTERFACE-NAME> – Clears detected spanning tree entries on a specified interface. Specify the interface name. • ge <1-5> – Clears detected spanning tree entries for the selected GigabitEthernet interface. Select the GigabitEthernet interface index from 1 - 5. • me1 – Clears FastEthernet interface status • port-channel <1-3> – Clears detected spanning tree entries for the selected port channel interface. Select the port channel index from 1 - 3. • pppoe1 – Clears detected spanning tree entries for PPPoE interface. • vlan <1-4094> – Clears detected spanning tree entries for the selected VLAN interface. Select a SVI VLAN ID from 1- 4094. • wwan1 – Clears detected spanning tree entries for wireless WAN interface
on <DEVICE-NAME>	Optional. Clears spanning tree protocol entries on a selected device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
clear vrrp [error-stats|stats] {on <DEVICE-NAME>}
```

vrrp	Clears *Virtual Router Redundancy Protocol* (VRRP) statistics for a device
error-stats {on <DEVICE-NAME>}	Clears global error statistics • on <DEVICE-NAME> – Optional. Clears VRRP global error statistics on a selected device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.
stats {on <DEVICE-NAME>}	Clears VRRP related statistics • on <DEVICE-NAME> – Optional. Clears VRRP related statistics on a selected device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Example

```
rfs7000-37FABE#clear crypto isakmp sa 111.222.333.01 on rfs7000-37FABE
rfs7000-37FABE#

rfs7000-37FABE#clear spanning-tree detected-protocols interface port-channel 1
on rfs7000-37FABE
rfs7000-37FABE#

rfs7000-37FABE#clear ip dhcp bindings 172.16.10.9 on rfs7000-37FABE
rfs7000-37FABE#

rfs7000-37FABE#clear cdp neighbors on rfs7000-37FABE
rfs7000-37FABE#

rfs4000-229D58#clear spanning-tree detected-protocols interface ge 1
rfs4000-229D58#

rfs4000-229D58#clear lldp neighbors
rfs4000-229D58#

rfs4000-229D58#show event-history
EVENT HISTORY REPORT
Generated on '2013-02-15 14:40:22 UTC' by 'admin'

2013-01-31 01:07:59     rfs4000-229D58  SYSTEM     CLOCK_RESET          System
clock reset, Time: 2013-02-15 14:25:35
2013-01-31 01:06:24     rfs4000-229D58  SYSTEM     UI_USER_AUTH_SUCCESS UI user
'admin' from: '192.168.100.224' authentication successful
2013-01-31 00:58:28     rfs4000-229D58  SYSTEM     CONFIG_COMMIT
Configuration commit by user 'admin' from '192.168.100.225'
```

```
2013-01-31 00:49:54     rfs4000-229D58  SYSTEM     LOGIN
Successfully logged in user 'admin' with privilege 'superuser' from 'ssh'
2013-01-31 00:49:31     rfs4000-229D58  SYSTEM     LOGOUT              Logged
out user 'admin' with privilege 'superuser' from '192.168.100.225'
2013-01-31 00:16:32     rfs4000-229D58  SYSTEM     LOGOUT              Logged
out user 'admin' with privilege 'superuser' from '192.168.100.224(web)'
2013-01-31 00:15:36     rfs4000-229D58  SYSTEM     LOGIN
Successfully logged in user 'admin' with privilege 'superuser' from 'ssh'
2013-01-30 23:43:10     rfs4000-229D58  SYSTEM     UI_USER_AUTH_SUCCESS UI user
'admin' from: '192.168.100.224' authentication successful
2013-01-30 03:47:47     rfs4000-229D58  SYSTEM     LOGOUT              Logged
out user 'admin' with privilege 'superuser' from '192.168.100.231(web)'
2013-01-30 02:45:08     rfs4000-229D58  SYSTEM     UI_USER_AUTH_SUCCESS UI user
'admin' from: '192.168.100.231' authentication successful
--More--
rfs4000-229D58#

rfs4000-229D58#clear event-history

rfs4000-229D58#show event-history
EVENT HISTORY REPORT
Generated on '2013-02-15 14:42:51 UTC' by 'admin'

rfs4000-229D58#

nx4500-5CFA2B#show mac-address-table
------------------------------------------------------------
 BRIDGE VLAN PORT             MAC               STATE
------------------------------------------------------------
 1      1    up1              00-15-70-38-06-49 forward
 1      1    up1              00-0F-8F-19-BA-4C forward
 1      1    up1              B4-C7-99-5C-FA-8E forward
 1      1    up1              00-15-70-81-74-2D forward
 1      1    up1              00-23-68-0F-43-D8 forward
 1      1    up1              00-A0-F8-68-D5-64 forward
 1      1    up1              B4-C7-99-6C-88-09 forward
 1      1    up1              5C-0E-8B-18-10-91 forward
 1      1    up1              00-02-B3-28-D1-55 forward
 1      1    up1              3C-CE-73-F4-47-83 forward
 1      1    up1              00-15-70-37-FD-F2 forward
 1      1    up1              B4-C7-99-58-72-58 forward
 1      1    up1              B4-C7-99-71-17-28 forward
 1      1    up1              00-23-68-13-9B-34 forward
------------------------------------------------------------
Total number of MACs displayed: 14
nx4500-5CFA2B#

nx4500-5CFA2B#clear mac-address-table vlan 1

nx4500-5CFA2B#show mac-address-table
------------------------------------------------------------
 BRIDGE VLAN PORT             MAC               STATE
------------------------------------------------------------
 1      1    up1              00-15-70-38-06-49 forward
 1      1    up1              00-0F-8F-19-BA-4C forward
 1      1    up1              B4-C7-99-5C-FA-8E forward
 1      1    up1              00-15-70-81-74-2D forward
 1      1    up1              00-23-68-0F-43-D8 forward
 1      1    up1              00-A0-F8-68-D5-64 forward
 1      1    up1              B4-C7-99-6C-88-09 forward
```

```
 1      1    up1              B4-C7-99-58-72-58 forward
 1      1    up1              B4-C7-99-71-17-28 forward
-------------------------------------------------------
Total number of MACs displayed: 9
nx4500-5CFA2B#
```

clock

Privileged Exec Mode Commands

Sets a device's system clock

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
clock set <HH:MM:SS> <1-31> <MONTH> <1993-2035> {on <DEVICE-NAME>}
```

Parameters

```
clock set <HH:MM:SS> <1-31> <MONTH> <1993-2035> {on <DEVICE-NAME>}
```

clock set	Sets a device's system clock
<HH:MM:SS>	Sets the current time (in military format hours, minutes and seconds)
<1-31>	Sets the numerical day of the month
<MONTH>	Sets the month of the year from Jan - Dec
<1993-2035>	Sets a valid four digit year from 1993 - 2035
on <DEVICE-NAME>	Optional. Sets the clock on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Example

```
rfs4000-229D58#clock set 14:45:30 15 Feb 2013
rfs4000-229D58#

rfs4000-229D58#show clock
2013-02-15 14:45:43 UTC
rfs4000-229D58#
```

cluster

Privileged Exec Mode Commands

Initiates the cluster context. The cluster context provides centralized management to configure all cluster members from any one member.

Commands executed under this context are executed on all members of the cluster.

Supported in the following platforms:

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
cluster start-election
```

Parameters

```
cluster start-election
```

start-election	Starts a new cluster master election

Example

```
rfs7000-37FABE#cluster start-election
rfs7000-37FABE#
```

Related Commands:

create-cluster	Creates a new cluster on a specified device
join-cluster	Adds a controller, as cluster member, to an existing cluster of devices

configure

Privileged Exec Mode Commands

Enters the configuration mode. Use this command to enter the current device's configuration mode, or enable configuration from the terminal.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
configure {self|terminal}
```

Parameters

```
configure {self|terminal}
```

self	Optional. Enables the current device's configuration mode
terminal	Optional. Enables configuration from the terminal

Example

```
rfs7000-37FABE#configure self
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#

rfs7000-37FABE#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
rfs7000-37FABE(config)#
```

connect

Privileged Exec Mode Commands

Begins a console connection to a remote device using the remote device's MiNT ID or name

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
connect [mint-id <MINT-ID>|<REMOTE-DEVICE-NAME>]
```

Parameters

```
connect [mint-id <MINT-ID>|<REMOTE-DEVICE-NAME>]
```

mint-id <MINT-ID>	Connects to a remote system using the MiNT ID • <MINT-ID> – Specify the remote device's MiNT ID.
<REMOTE-DEVICE-NAME>	Connects to a remote system using its name • <REMOTE-DEVICE-NAME> – Specify the remote device's name.

Example

```
rfs4000-229D58#show mint lsp-db
1 LSPs in LSP-db of 68.22.9D.58:
LSP 68.22.9D.58 at level 1, hostname "rfs4000-229D58", 0 adjacencies, seqnum
1073
rfs4000-229D58#

rfs4000-229D58#connect mint-id 68.22.9D.58

Entering character mode
Escape character is '^]'.

Brocade Mobility RFS4000 release 5.5.0.0-018D
rfs4000-229D58 login: admin
Password:
rfs4000-229D58>
```

copy

Privileged Exec Mode Commands

Copies a file (config,log,txt...etc) from any location to the access point, wireless controller, or service platform and vice-versa

NOTE
Copying a new config file to an existing running-config file merges it with the existing running-config file on the wireless controller. Both the existing running-config and the new config file are applied as the current running-config.

Copying a new config file to a start-up config file replaces the existing start-up config file with the parameters of the new file. It is better to erase the existing start-up config file and then copy the new config file to the startup config.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
copy [<SOURCE-FILE>|<SOURCE-URL>] [<DESTINATION-FILE>|<DESTINATION-URL>]
```

Parameters

```
copy [<SOURCE-FILE>|<SOURCE-URL>] [<DESTINATION-FILE>|<DESTINATION-URL>]
```

<SOURCE-FILE>	Specify the source file to copy.
<SOURCE-URL>	Specify the source file's location (URL).
<DESTINATION-FILE>	Specify the destination file to copy to.
<DESTINATION-URL>	Specify the destination file's location (URL).

Example

```
Transferring file snmpd.log to remote TFTP server.
rfs7000-37FABE#copy flash:/log/snmpd.log
tftp://157.235.208.105:/snmpd.log
Accessing running-config file from remote TFTP server into switch
running-config.
rfs7000-37FABE#copy tftp://157.235.208.105:/running-config running-config
```

create-cluster

Privileged Exec Mode Commands

Creates a new device cluster, with the specified name, and assigns it an IP address and routing level

A cluster (or redundancy group) is a set of controllers or service platforms (nodes) uniquely defined by a profile configuration. Within the cluster, members discover and establish connections to other members and provide wireless network self-healing support in the event of member's failure.

A cluster's load balance is typically distributed evenly amongst its members. An administrator needs to define how often the profile is load balanced for radio distribution, as radios can come and go and members join and exit the cluster.

Supported in the following platforms:

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
create-cluster name <CLUSTER-NAME> ip <IP> {level [1|2]}
```

Parameters

```
create-cluster name <CLUSTER-NAME> ip <IP> {level [1|2]}
```

create-cluster	Creates a cluster
name <CLUSTER-NAME>	Configures the cluster name • <CLUSTER-NAME> – Specify a cluster name. Define a name for the cluster name unique to its configuration or profile support requirements. The name cannot exceed 64 characters.
ip <IP>	Specifies the device's IP address used for cluster creation • <IP> – Specify the device's IP address in the A.B.C.D format.
level [1|2]	Optional. Configures the routing level for this cluster • 1 – Configures level 1 (local) routing • 2 – Configures level 2 (inter-site) routing

Example

```
rfs7000-37FABE>create-cluster name Cluster1 ip 172.16.10.1 level 1
... creating cluster
... committing the changes
... saving the changes
[OK]
rfs7000-37FABE>

nx6500-31FABE>create-cluster <CLUSTER-NAME>
```

Related Commands:

cluster	Initiates the cluster context. The cluster context provides centralized management to configure all cluster members from any one member.
join-cluster	Adds a wireless controller, access point, or service platform, as cluster member, to an existing cluster of devices

crypto

Privileged Exec Mode Commands

Enables digital certificate configuration and RSA Keypair management. Digital certificates are issued by *Certificate Authorities* (CAs) and contain user or device specific information, such as name, public key, IP address, serial number, company name etc. Use this command to generate, delete, export, or import encrypted RSA Keypairs and generate *Certificate Signing Request* (CSR).

This command also enables trustpoint configuration. Trustpoints contain the CA's identity and configuration parameters.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
crypto [key|pki]

crypto key [export|generate|import|zeroize]

crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL>
{background|on|passphrase}
crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL>
          {background {on <DEVICE-NAME>}|on <DEVICE-NAME>}
crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL>
          {passphrase <KEY-PASSPHRASE> {background {on <DEVICE-NAME>}|on
<DEVICE-NAME>}}

crypto key generate rsa <RSA-KEYPAIR-NAME> <1024-2048> {on <DEVICE-NAME>}

crypto key import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL>
{background|on|passphrase}
crypto key import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL>
          {background {on <DEVICE-NAME>}|on <DEVICE-NAME>}
crypto key import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL>
          {passphrase <KEY-PASSPHRASE> {background {on <DEVICE-NAME>}|on
<DEVICE-NAME>}}

crypto key zeroize rsa <RSA-KEYPAIR-NAME> {force {on <DEVICE-NAME>}|on
<DEVICE-NAME>}

crypto pki [authenticate|export|generate|import|zeroize]

crypto pki authenticate <TRUSTPOINT-NAME> <LOCATION-URL>
          {background {on <DEVICE-NAME>}|on <DEVICE-NAME>}

crypto pki export [request|trustpoint]
crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME>
          [autogen-subject-name|subject-name]
crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME>
   autogen-subject-name (<EXPORT-TO-URL>,email <SEND-TO-EMAIL>,fqdn <FQDN>,
   ip-address <IP>)
crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME>
   autogen-subject-name <EXPORT-TO-URL> {background {on <DEVICE-NAME>}|
   on <DEVICE-NAME>}
crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME>
          subject-name <COMMON-NAME> <COUNTRY> <STATE> <CITY> <ORGANIZATION>
   <ORGANIZATION-UNIT> (<EXPORT-TO-URL>,email <SEND-TO-EMAIL>,fqdn <FQDN>,
   ip-address <IP>)]
```

```
crypto pki export trustpoint <TRUSTPOINT-NAME> <EXPORT-TO-URL> {background
  {on <DEVICE-NAME>}|on <DEVICE-NAME>|passphrase <KEY-PASSPHRASE> {background
  {on <DEVICE-NAME>}|on <DEVICE-NAME>}}

crypto pki generate self-signed <TRUSTPOINT-NAME> [generate-rsa-key|
  use-rsa-key] <RSA-KEYPAIR-NAME> [autogen-subject-name|subject-name]
crypto pki generate self-signed <TRUSTPOINT-NAME>
[generate-rsa-key|use-rsa-key]
          <RSA-KEYPAIR-NAME> autogen-subject-name {(email
<SEND-TO-EMAIL>,fqdn <FQDN>,
          ip-address <IP>,on <DEVICE-NAME>)}
crypto pki generate self-signed <TRUSTPOINT-NAME>
[generate-rsa-key|use-rsa-key]
          <WORD> subject-name <COMMON-NAME> <COUNTRY> <STATE> <CITY>
<ORGANIZATION>
          <ORGANIZATION-UNIT> {(email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address
<IP>,
          on <DEVICE-NAME>)}

crypto pki import [certificate|crl|trustpoint]
crypto pki import [certificate|crl] <TRUSTPOINT-NAME> <IMPORT-FROM-URL>
  {background {on <DEVICE-NAME>}|on <DEVICE-NAME>}]
crypto pki import trustpoint <TRUSTPOINT-NAME> <IMPORT-FROM-URL>
  {background {on <DEVICE-NAME>}|on <DEVICE-NAME>|passphrase <KEY-PASSPHRASE>
  {background {on <DEVICE-NAME>}|on <DEVICE-NAME>}}

crypto pki zeroize trustpoint <TRUSTPOINT-NAME> {del-key {on <DEVICE-NAME>}|
  on <DEVICE-NAME>}
```

Parameters

```
crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL>
{background {on <DEVICE-NAME>}|on <DEVICE-NAME>}
```

key	Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.
export rsa <RSA-KEYPAIR-NAME>	Exports an existing RSA Keypair to a specified destination • <RSA-KEYPAIR-NAME> – Specify the RSA Keypair name.
<EXPORT-TO-URL>	Specify the RSA Keypair destination address in the following format: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb<n>:/path/file
background {on <DEVICE-NAME>}	Optional. Performs an export operation in the background. Optionally specify the device to export to.
on <DEVICE-NAME>	Optional. Performs an export operation on a specific device. • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL> {passphrase
<KEY-PASSPHRASE> {background {on <DEVICE-NAME>}|on <DEVICE-NAME>}}
```

key	Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.
export rsa	Exports a RSA Keypair to a specified destination • <RSA-KEYPAIR-NAME> – Specify the RSA Keypair name.

<EXPORT-TO-URL> {passphrase <KEY-PASSPHRASE>}	Specify the RSA Keypair destination address in the following format: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb<n>:/path/file • passphrase – Optional. Encrypts RSA Keypair before exporting • <KEY-PASSPHRASE> – Specify a passphrase to encrypt the RSA Keypair.
on <DEVICE-NAME>	Optional. Performs an export operation on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`crypto key generate rsa <RSA-KEYPAIR-NAME> <1024-2048> {on <DEVICE-NAME>}`

key	Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.
generate rsa <RSA-KEYPAIR-NAME> <1024-2048>	Generates a new RSA Keypair • <RSA-KEYPAIR-NAME> – Specify the RSA Keypair name. • <1024-2048> – Sets the size of the RSA key in bits from 1024 - 2048. The default size is 1024.
on <DEVICE-NAME>	Optional. Generates the new RSA Keypair on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`crypto key import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL> {background {on <DEVICE-NAME>}|on <DEVICE-NAME>}`

key	Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.
import rsa <RSA-KEYPAIR-NAME>	Imports a RSA Keypair from a specified source • <RSA-KEYPAIR-NAME> – Specify the RSA Keypair name.
<IMPORT-FROM-URL>	Specify the RSA Keypair source address in the following format: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb<n>:/path/file
on <DEVICE-NAME>	Optional. Performs an import operation on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.
background {on <DEVICE-NAME>}	Optional. Performs an import operation in the background • on <DEVICE-NAME> – Optional. Performs import operation on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`crypto key import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL> {passphrase <KEY-PASSPHRASE> {background {on <DEVICE-NAME>}|on <DEVICE-NAME>}}`

key	Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.
import rsa <RSA-KEYPAIR-NAME>	Decrypts and imports a RSA Keypair from a specified source • <RSA-KEYPAIR-NAME> – Specify the RSA Keypair name.

<IMPORT-FROM-URL> {passphrase <KEY-PASSPHRASE>}	Specify the RSA Keypair source address in the following format: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb<n>:/path/file • passphrase – Optional. Decrypts the RSA Keypair before importing it • <KEY-PASSPHRASE> – Specify the passphrase to decrypt the RSA Keypair.
on <DEVICE-NAME>	Optional. Performs import operation on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`crypto key zeroize rsa <RSA-KEYPAIR-NAME> {force {on <DEVICE-NAME>}|on <DEVICE-NAME>}`

key	Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.
zeroize rsa <RSA-KEYPAIR-NAME>	Deletes a specified RSA Keypair • <RSA-KEYPAIR-NAME> – Specify the RSA Keypair name. **NOTE:** All device certificates associated with this key will also be deleted.
force {on <DEVICE-NAME>}	Optional. Forces deletion of all certificates associated with the specified RSA Keypair. Optionally specify a device on which to force certificate deletion.
on <DEVICE-NAME>	Optional. Deletes all certificates associated with the RSA Keypair on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`crypto pki authenticate <TRUSTPOINT-NAME> <URL> {background {on <DEVICE-NAME>}|on <DEVICE-NAME>}`

pki	Enables *Private Key Infrastructure* (PKI) management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.
authenticate <TRUSTPOINT-NAME>	Authenticates a trustpoint and imports the corresponding CA certificate <TRUSTPOINT-NAME> – Specify the trustpoint name.
<URL>	Specify CA's location in the following format: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb<n>:/path/file **NOTE:** The CA certificate is imported from the specified location.
background {on <DEVICE-NAME>}	Optional. Performs authentication in the background. Optionally specify a device on which to perform authentication.
on <DEVICE-NAME>	Optional. Performs authentication on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

	`crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME> autogen-subject-name (url <EXPORT-TO-URL>,email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address <IP>)`
pki	Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.
export request	Exports CSR to the CA for digital identity certificate. The CSR contains applicant's details and RSA Keypair's public key.
[generate-rsa-key| use-rsa-key] <RSA-KEYPAIR-NAME>	Generates a new RSA Keypair or uses an existing RSA Keypair • generate-rsa-key – Generates a new RSA Keypair for digital authentication • use-rsa-key – Uses an existing RSA Keypair for digital authentication • <RSA-KEYPAIR-NAME> – If generating a new RSA Keypair, specify a name for it. If using an existing RSA Keypair, specify its name.
autogen-subject-name	Auto generates subject name from configuration parameters. The subject name identifies the certificate.
url <EXPORT-TO-URL> {background {on <DEVICE-NAME}| on <DEVICE-NAME>}	Specify the CA's location in the following format: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb<n>:/path/file **NOTE:** The CSR is exported to the specified location. • background – Optional. Performs export operation in the background • on <DEVICE-NAME> – Optional. Performs export operation on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.
email <SEND-TO-EMAIL>	Exports CSR to a specified e-mail address • <SEND-TO-EMAIL> – Specify the CA's e-mail address.
fqdn <FQDN>	Exports CSR to a specified *Fully Qualified Domain Name* (FQDN) • <FQDN> – Specify the CA's FQDN.
ip address <IP>	Exports CSR to a specified device or system • <IP> – Specify the CA's IP address.

	`crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME> subject-name <COUNTRY> <STATE> <CITY> <ORGANIZATION> <ORGANIZATION-UNIT> (<EXPORT-TO-URL>,email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address <IP>)`
pki	Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.
export request	Exports CSR to the CA for a digital identity certificate.The CSR contains applicant's details and RSA Keypair's public key.
[generate-rsa-key| use-rsa-key] <RSA-KEYPAIR-NAME>	Generates a new RSA Keypair or uses an existing RSA Keypair • generate-rsa-key – Generates a new RSA Keypair for digital authentication • use-rsa-key – Uses an existing RSA Keypair for digital authentication • <RSA-KEYPAIR-NAME> – If generating a new RSA Keypair, specify a name for it. If using an existing RSA Keypair, specify its name.
subject-name <COMMON-NAME>	Specifies subject name to identify the certificate • <COMMON-NAME> – Sets the common name used with the CA certificate. The name should enable you to identify the certificate easily (2 to 64 characters in length).
<COUNTRY>	Sets the deployment country code (2 character ISO code)
<STATE>	Sets the state name (2 to 64 characters in length)
<CITY>	Sets the city name (2 to 64 characters in length)

<ORGANIZATION>	Sets the organization name (2 to 64 characters in length)
<ORGANIZATION-UNIT>	Sets the organization unit (2 to 64 characters in length)
<EXPORT-TO-URL> {background {on <DEVICE-NAME}| on <DEVICE-NAME>}	Specify the CA's location in the following format: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb<n>:/path/file **NOTE:** The CSR is exported to the specified location. • background – Optional. Performs an export operation in the background • on <DEVICE-NAME> – Optional. Performs an export operation on a specific device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.
email <SEND-TO-EMAIL>	Exports CSR to a specified e-mail address • <SEND-TO-EMAIL> – Specify the CA's e-mail address.
fqdn <FQDN>	Exports CSR to a specified FQDN • <FQDN> – Specify the CA's FQDN.
ip address <IP>	Exports CSR to a specified device or system • <IP> – Specify the CA's IP address.

`crypto pki export trustpoint <TRUSTPOINT-NAME> <EXPORT-TO-URL> {background {on <DEVICE-NAME>}|on <DEVICE-NAME>|passphrase <KEY-PASSPHRASE> background {on <DEVICE-NAME>}|on <DEVICE-NAME>}}`

pki	Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.
export trustpoint <TRUSTPOINT-NAME>	Exports a trustpoint along with CA certificate, *Certificate Revocation List* (CRL), server certificate, and private key • <TRUSTPOINT-NAME> – Specify the trustpoint name.
<EXPORT-TO-URL>	Specify the destination address in the following format: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb<n>:/path/file
background {on <DEVICE-NAME>}	Optional. Performs an export operation in the background • on <DEVICE-NAME> – Optional. Performs an export operation on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.
on <DEVICE-NAME>	Optional. Performs an export operation on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.
passphrase <KEY-PASSPHRASE> {background {on <DEVICE-NAME>}| on <DEVICE-NAME>}	Optional. Encrypts the key with a passphrase before exporting • <KEY-PASSPHRASE> – Specify the passphrase. • background – Optional. Performs export operation in the background • on <DEVICE-NAME> – Optional. Performs export operation on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
crypto pki generate self-signed <TRUSTPOINT-NAME>
[generate-rsa-key|use-rsa-key]
<RSA-KEYPAIR-NAME> autogen-subject-name {(email <SEND-TO-EMAIL>,fqdn
<FQDN>,ip-address <IP>,on <DEVICE-NAME>)}
```

pki	Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.
generate	Generates a CA certificate and a trustpoint
self-signed <TRUSTPOINT-NAME>	Generates a self-signed CA certificate and a trustpoint • <TRUSTPOINT-NAME> – Specify a name for the certificate and its trustpoint.
[generate-rsa-key| use-rsa-key] <RSA-KEYPAIR-NAME>	Generates a new RSA Keypair, or uses an existing RSA Keypair • generate-rsa-key – Generates a new RSA Keypair for digital authentication • use-rsa-key – Uses an existing RSA Keypair for digital authentication • <RSA-KEYPAIR-NAME> – If generating a new RSA Keypair, specify a name for it. If using an existing RSA Keypair, specify its name.
autogen-subject-name	Auto generates the subject name from the configuration parameters. The subject name helps to identify the certificate
email <SEND-TO-EMAIL>	Optional. Exports CSR to a specified e-mail address • <SEND-TO-EMAIL> – Specify the CA's e-mail address.
fqdn <FQDN>	Optional. Exports CSR to a specified FQDN • <FQDN> – Specify the CA's FQDN.
ip-address <IP>	Optional. Exports CSR to a specified device or system • <IP> – Specify the CA's IP address.
on <DEVICE-NAME>	Optional. Exports the CSR on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
crypto pki generate self-signed <TRUSTPOINT-NAME>
[generate-rsa-key|use-rsa-key]
<RSA-KEYPAIR-NAME> subject-name <COMMON-NAME> <COUNTRY> <STATE> <CITY>
<ORGANIZATION> <ORGANIZATION-UNIT> {(email <SEND-TO-EMAIL>,fqdn
<FQDN>,ip-address <IP>,on <DEVICE-NAME>)}
```

pki	Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.
generate self-signed <TRUSTPOINT-NAME>	Generates a self-signed CA certificate and a trustpoint • <TRUSTPOINT-NAME> – Specify a name for the certificate and its trustpoint.
[generate-rsa-key| use-rsa-key] <RSA-KEYPAIR-NAME>	Generates a new RSA Keypair, or uses an existing RSA Keypair • generate-rsa-key – Generates a new RSA Keypair for digital authentication • use-rsa-key – Uses an existing RSA Keypair for digital authentication • <RSA-KEYPAIR-NAME> – If generating a new RSA Keypair, specify a name for it. If using an existing RSA Keypair, specify its name.
subject-name <COMMON-NAME>	Specify a subject name to identify the certificate. • <COMMON-NAME> – Specify the common name used with the CA certificate. The name should enable you to identify the certificate easily.
<COUNTRY>	Sets the deployment country code (2 character ISO code)
<STATE>	Sets the state name (2 to 64 characters in length)
<CITY>	Sets the city name (2 to 64 characters in length)
<ORGANIZATION>	Sets the organization name (2 to 64 characters in length)
<ORGANIZATION-UNIT>	Sets the organization unit (2 to 64 characters in length)

email <SEND-TO-EMAIL>	Optional. Exports the CSR to a specified e-mail address • <SEND-TO-EMAIL> – Specify the CA's e-mail address.
fqdn <FQDN>	Optional. Exports the CSR to a specified FQDN • <FQDN> – Specify the CA's FQDN.
ip address <IP>	Optional. Exports the CSR to a specified device or system • <IP> – Specify the CA's IP address.
on <DEVICE-NAME>	Optional. Exports the CSR on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`crypto pki import [certificate|crl] <TRUSTPOINT-NAME> <IMPORT-FROM-URL>`
`{background {on <DEVICE-NAME>}|on <DEVICE--NAME>}`

pki	Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.
import	Imports certificates, CRL, or a trustpoint to the selected device
[certificate|crl] <TRUSTPOINT-NAME>	Imports a signed server certificate or CRL • certificate – Imports signed server certificate • crl – Imports CRL • <TRUSTPOINT-NAME> – Specify the trustpoint name (should be authenticated).
<IMPORT-FROM-URL>	Specify the signed server certificate or CRL source address in the following format: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb<n>:/path/file
background {on <DEVICE-NAME>}	Optional. Performs import operation in the background • on <DEVICE-NAME> – Optional. Performs import operation on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.
on <DEVICE-NAME>	Optional. Performs import operation on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`crypto pki import trustpoint <TRUSTPOINT-NAME> <IMPORT-FROM-URL>`
`{background {on <DEVICE-NAME>}|on <DEVICE-NAME>|passphrase <KEY-PASSPHRASE>`
`{background {on <DEVICE-NAME>}|on <DEVICE-NAME>}}`

pki	Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.
import	Imports certificates, CRL, or a trustpoint to the selected device
trustpoint <TRUSTPOINT-NAME>	Imports a trustpoint and its associated CA certificate, server certificate, and private key • <TRUSTPOINT-NAME> – Specify the trustpoint name (should be authenticated).
<IMPORT-FROM-URL>	Specify the trustpoint source address in the following format: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb<n>:/path/file

background {on <DEVICE-NAME>}	Optional. Performs import operation in the background • on <DEVICE-NAME> – Optional. Performs import operation on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.
on <DEVICE-NAME>	Optional. Performs import operation on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.
passphrase <KEY-PASSPHRASE> {background {on <DEVICE-NAME>}| on <DEVICE-NAME>}	Optional. Encrypts trustpoint with a passphrase before importing it • <KEY-PASSPHRASE> – Specify a passphrase. • background – Optional. Imports the encrypted trustpoint in the background • on <DEVICE-NAME> – Optional. Imports the encrypted trustpoint on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`crypto pki zeroize trustpoint <TRUSTPOINT-NAME> {del-key {on <DEVICE-NAME>}| on <DEVICE-NAME>}`

pki	Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.
zeroize <TRUSTPOINT-NAME>	Deletes a trustpoint and its associated CA certificate, server certificate, and private key • <TRUSTPOINT-NAME> – Specify the trustpoint name (should be authenticated).
del-key {on <DEVICE-NAME>}	Optional. Deletes the private key associated with the server certificate • on <DEVICE-NAME> – Optional. Deletes private key on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.
on <DEVICE-NAME>	Optional. Deletes the trustpoint on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Example

```
rfs7000-37FABE#crypto key generate rsa key 1025
RSA Keypair successfully generated
rfs7000-37FABE#

rfs7000-37FABE#crypto key import rsa moto123 url passphrase word background on
rfs7000-37FABE
RSA key import operation is started in background
rfs7000-37FABE#

rfs7000-37FABE#crypto pki generate self-signed word generate-rsa-key word
autogen-subject-name fqdn word
Successfully generated self-signed certificate
rfs7000-37FABE#

rfs7000-37FABE#crypto pki zeroize trustpoint word del-key on rfs7000-37FABE
Successfully removed the trustpoint and associated certificates
%Warning: Applications associated with the trustpoint will start using
default-trustpoint
rfs7000-37FABE#

rfs7000-37FABE#crypto pki authenticate word url background on rfs7000-37FABE
Import of CA certificate started in background
rfs7000-37FABE#

rfs7000-37FABE#crypto pki import trustpoint word url passphrase word on
rfs7000-37FABE
Import operation started in background
rfs7000-37FABE#
```

Related Commands:

no	Removes server certificates, trustpoints and their associated certificates

delete

Privileged Exec Mode Commands

Deletes a specified file from the device's file system

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
delete [/force <FILE>|/recursive <FILE>|<FILE>]
```

Parameters

```
delete [/force <FILE>|/recursive <FILE>|<FILE>]
```

/force <FILE>	Forces deletion without a prompt
/recursive <FILE>	Performs a recursive delete
<FILE>	Specifies the file name • Deletes the file specified by the <FILE> parameter

Example

```
rfs7000-37FABE#delete flash:/out.tar flash:/out.tar.gz
Delete flash:/out.tar [y/n]? y
Delete flash:/out.tar.gz [y/n]? y

rfs7000-37FABE#delete /force flash:/tmp.txt
rfs7000-37FABE#

rfs7000-37FABE#delete /recursive flash:/backup/
Delete flash:/backup//fileMgmt_350_180B.core

[y/n]? y
Delete

flash:/backup//fileMgmt_350_18212X.core_bk

[y/n]? n

Delete flash:/backup//imish_1087_18381X.core.gz

[y/n]? n
rfs7000-37FABE#
```

device-upgrade

Privileged Exec Mode Commands

Enables firmware upgrade on an adopted device or a set of adopted devices (access points, wireless controllers, and service platforms)

This command simplifies device upgradation within a *hierarchically managed* (HM) network. For more information on HM networks, see *device-upgrade*.

NOTE
A NOC controller's capacity is equal to, or higher than that of a site controller. The following devices can be deployed at NOC and sites:
- NOC controller – Brocade Mobility RFS7000 and Brocade Mobility RFS9510
- Site controller – Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
Within a HM network, the devices deployed as site controllers depends on the NOC controller device type. For more information on the adoption capabilities of various NOC controller devices, see Usage Guidelines *(NOC controller adoption matrix)*.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
device-upgrade [<MAC/HOSTNAME>|all|br650|br6511|br1220|
          |br71xx|br81xx|rfs4000|rfs6000|rfs7000|
          cancel-upgrade|load-image|rf-domain]

device-upgrade <MAC/HOSTNAME> {no-reboot|reboot-time <TIME>|
          upgrade-time <TIME> {no-reboot|reboot-time <TIME>}}

device-upgrade all {no-reboot|reboot-time <TIME>|upgrade-time <TIME>
{no-reboot|
          reboot-time <TIME>}} {(staggered-reboot)}

device-upgrade [br650|br6511|br1220|br71xx|br81xx|
          rfs4000|rfs6000|rfs7000] all
          {no-reboot|reboot-time <TIME>|upgrade-time <TIME>
{no-reboot|reboot-time <TIME>}}
          {(staggered-reboot)}

device-upgrade cancel-upgrade [<MAC/HOSTNAME>|all|br650|br6511|
          br1220|br71xx|br81xx|rfs4000|rfs6000|rfs7000|on]
```

```
device-upgrade cancel-upgrade [<MAC/HOSTNAME>|all]

device-upgrade cancel-upgrade [br650|br6511|br1220|
          br71xx|br81xx|rfs4000|rfs6000|rfs7000] all
device-upgrade cancel-upgrade on rf-domain [<RF-DOMAIN-NAME>|all]

device-upgrade load-image [br650|br6511|br1220|
          br71xx|br81xx|rfs4000|rfs6000|rfs7000] <IMAGE-URL>

device-upgrade rf-domain [<RF-DOMAIN-NAME>|all] [all|br650|br6511|
          br1220|br71xx|br81xx|rfs4000|rfs6000|rfs7000]
{<MAC/HOSTNAME>|no-reboot|from-controller|reboot-time <TIME>|
          staggered-reboot|upgrade-time <TIME>}

device-upgrade rf-domain [<RF-DOMAIN-NAME>|all] [all|br650|br6511|br1220|
          br71xx|br81xx|rfs4000|rfs6000|rfs7000]
{<MAC/HOSTNAME>|no-reboot|reboot-time <TIME>} {(staggered-reboot)}

device-upgrade rf-domain [<RF-DOMAIN-NAME>|all] [all|br650|br6511|
          |br71xx|br81xx|rfs4000|rfs6000|rfs7000]
          {from-controller {no-reboot|reboot-time <TIME>|upgrade-time <TIME>
          {no-reboot|reboot-time <TIME>}} {(staggered-reboot)}

device-upgrade rf-domain [<RF-DOMAIN-NAME>|all] [all|br650|br6511|
          br1220|br71xx|br81xx|rfs4000|rfs6000|rfs7000] {upgrade-time <TIME>
{no-reboot|reboot-time <TIME>}} {(staggered-reboot)}
```

Parameters

```
device-upgrade <MAC/HOSTNAME> {no-reboot|reboot-time <TIME>|upgrade-time
<TIME>
{no-reboot|reboot-time <TIME>}}
```

<MAC/HOSTNAME>	Upgrades firmware on the device identified by the <MAC/HOSTNAME> keyword • <MAC/HOSTNAME> – Specify the device's MAC address or hostname.
no-reboot	Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)
reboot-time <TIME>	Optional. Schedules an automatic reboot after a successful upgrade • <TIME> – Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.
upgrade-time <TIME> {no-reboot| reboot-time <TIME>}	Optional. Schedules an automatic device firmware upgrade • <TIME> – Specify the upgrade time in the MM/DD/YYYY-HH:MM or HH:MM format. The following actions can be performed after a scheduled upgrade: • no-reboot – Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted) • reboot-time <TIME> – Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.

```
device-upgrade all {no-reboot|reboot-time <TIME>|upgrade-time <TIME>
{no-reboot|
reboot-time <TIME>}} {(staggered-reboot)}
```

all	Upgrades firmware on all devices
no-reboot	Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)
reboot-time <TIME>	Optional. Schedules an automatic reboot after a successful upgrade • <TIME> – Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.

upgrade-time <TIME> {no-reboot| reboot-time <TIME>}	Optional. Schedules an automatic device firmware upgrade on all devices • <TIME> – Specify the upgrade time in the MM/DD/YYYY-HH:MM or HH:MM format. The following actions can be performed after a scheduled upgrade: • no-reboot – Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted) • reboot-time <TIME> – Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.
staggered-reboot	This keyword is common to all of the above. • Optional. Enables staggered reboot (one at a time), without network impact

`device-upgrade [br650|br6511|br1220|br71xx|br81xx| |rfs4000|rfs6000|rfs7000] all` *`{no-reboot|reboot-time <TIME>| upgrade-time <TIME> {no-reboot|reboot-time <TIME>}} {(staggered-reboot)}`*

[br650| br6511|br1220| br71xx| br81xx|rfs4000| rfs6000|rfs7000] all	Upgrades firmware on all devices of a specific type. Select the device type. • Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point • Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000 • Service Platforms — , Brocade Mobility RFS9510 • all – Upgrades firmware on all • Brocade Mobility 650 Access Point all – Upgrades firmware on all Brocade Mobility 650 Access Points • Brocade Mobility 6511 Access Point all – Upgrades firmware on all Brocade Mobility 6511 Access Points • Brocade Mobility 1220 Access Point all – Upgrades firmware on all Brocade Mobility 1220 Access Points • Brocade Mobility 71XX Access Point all – Upgrades firmware on all Brocade Mobility 71XX Access Points • Brocade Mobility 1240 Access Point all – Upgrades firmware on all Brocade Mobility 1240 Access Points • Brocade Mobility RFS4000 all – Upgrades firmware on all Brocade Mobility RFS4000s • Brocade Mobility RFS6000 all – Upgrades firmware on all Brocade Mobility RFS6000s • Brocade Mobility RFS7000 all – Upgrades firmware on all Brocade Mobility RFS7000s After selecting the device type, schedule an automatic upgrade and/or an automatic reboot.
no-reboot	Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)
reboot-time <TIME>	Optional. Schedules an automatic reboot after a successful upgrade • <TIME> – Optional. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.
upgrade-time <TIME> {no-reboot| reboot-time <TIME>}	Optional. Schedules an automatic firmware upgrade on all devices of the specified type • <TIME> – Specify the upgrade time in the MM/DD/YYYY-HH:MM or HH:MM format. The following actions can be performed after a scheduled upgrade: • no-reboot – Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted) • reboot-time <TIME> – Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.
staggered-reboot	This keyword is common to all of the above. • Optional. Enables staggered reboot (one at a time), without network impact

`device-upgrade cancel-upgrade [<MAC/HOSTNAME>|all]`

cancel-upgrade [<MAC/HOSTNAME>| all]	Cancels a scheduled firmware upgrade on a specified device or on all devices • <MAC/HOSTNAME> – Cancels a scheduled upgrade on the device identified by the <MAC/HOSTNAME> keyword. Specify the device's MAC address or hostname. • all – Cancels scheduled upgrade on all devices

	`device-upgrade cancel-upgrade [br650|br1220| br71xx|br81xx|rfs4000|rfs6000|rfs7000] all`
cancel-upgrade [br650| br6511|br1220|br71xx| br81xx|rfs4000| rfs6000|rfs7000] all	Cancels scheduled firmware upgrade on all devices of a specific type. Select the device type. • Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point • Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000 • Service Platforms — Brocade Mobility RFS9510 • all – Cancels scheduled upgrade on all • Brocade Mobility 650 Access Point all – Cancels scheduled upgrade on all Brocade Mobility 650 Access Points • Brocade Mobility 6511 Access Point all – Cancels scheduled upgrade on all Brocade Mobility 6511 Access Points • Brocade Mobility 1220 Access Point all – Cancels scheduled upgrade on all Brocade Mobility 1220 Access Points • Brocade Mobility 71XX Access Point all – Cancels scheduled upgrade on all Brocade Mobility 71XX Access Points • Brocade Mobility 1240 Access Point all – Cancels scheduled upgrade on all Brocade Mobility 1240 Access Points • Brocade Mobility RFS4000 all – Cancels scheduled upgrade on all Brocade Mobility RFS4000s • Brocade Mobility RFS6000 all – Cancels scheduled upgrade on all Brocade Mobility RFS6000s • Brocade Mobility RFS7000 all – Cancels scheduled upgrade on all Brocade Mobility RFS7000s

	`device-upgrade cancel-upgrade on rf-domain [<DOMAIN-NAME>|all]`
cancel-upgrade on rf-domain [<RF-DOMAIN-NAME>| all]	Cancels scheduled firmware upgrade in a specified RF Domain or all RF Domains • <RF-DOMAIN-NAME> – Cancels scheduled device upgrade in a specified RF Domain. Specify the RF Domain name. • all – Cancels scheduled device upgrades across all RF Domains

```
device-upgrade load-image [br650|br6511|br1220|
br71xx|br81xx|rfs4000|rfs6000|rfs7000] <IMAGE-URL>
```

load-image [br650|br6511|br1220|br71xx|br81xx|rfs4000|rfs6000|rfs7000]	Loads device firmware image from a specified location. Select the device type and provide the location of the required device firmware image. • Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point • Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000 • Service Platforms — Brocade Mobility RFS9510 • firmware image • Brocade Mobility 650 Access Point <IMAGE-URL> – Loads Brocade Mobility 650 Access Point firmware image • Brocade Mobility 6511 Access Point <IMAGE-URL> – Loads Brocade Mobility 6511 Access Point firmware image • Brocade Mobility 71XX Access Point <IMAGE-URL> – Loads Brocade Mobility 71XX Access Point firmware image • Brocade Mobility 1240 Access Point <IMAGE-URL> – Loads Brocade Mobility 1240 Access Point firmware image • Brocade Mobility RFS4000 <IMAGE-URL> – Loads Brocade Mobility RFS4000 firmware image • Brocade Mobility RFS6000 <IMAGE-URL> – Loads Brocade Mobility RFS6000 firmware image • Brocade Mobility RFS7000 <IMAGE-URL> – Loads Brocade Mobility RFS7000 firmware image
<IMAGE-URL>	Specify the device's firmware image location in one of the following formats: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>:<passwd>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb<n>:/path/file

```
device-upgrade rf-domain [<RF-DOMAIN-NAME>|all] [all|br650|br6511|
br1220|br71xx|br81xx|rfs4000|rfs6000|rfs7000]
{<MAC/HOSTNAME>|no-reboot|reboot-time <TIME>} {(staggered-reboot)}
```

rf-domain [<RF-DOMAIN-NAME>|all]	Upgrades firmware on devices in a specified RF Domain or all RF Domains. Devices within a RF Domain are upgraded through the RF Domain manager. • <RF-DOMAIN-NAME> – Upgrades devices in a specified RF Domain. Specify the RF Domain name. • all – Upgrades devices across all RF Domains
[all|br650|br6511|br1220|br71xx|br81xx|rfs4000|rfs6000|rfs7000]	After specifying the RF Domain, select the device type. • all – Upgrades firmware on all devices • Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point • Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000 • Service Platforms — Brocade Mobility RFS9510 • Brocade Mobility 650 Access Point – Upgrades firmware on all Brocade Mobility 650 Access Points • Brocade Mobility 6511 Access Point – Upgrades firmware on all Brocade Mobility 6511 Access Points • Brocade Mobility 1220 Access Point – Upgrades firmware on all Brocade Mobility 1220 Access Points • Brocade Mobility 71XX Access Point – Upgrades firmware on all Brocade Mobility 71XX Access Points • Brocade Mobility 1240 Access Point – Upgrades firmware on all Brocade Mobility 1240 Access Points • Brocade Mobility RFS4000 – Upgrades firmware on all Brocade Mobility RFS4000s • Brocade Mobility RFS6000 – Upgrades firmware on all Brocade Mobility RFS6000s • Brocade Mobility RFS7000 – Upgrades firmware on all Brocade Mobility RFS7000s
<MAC/HOSTNAME>	Optional. Upgrades firmware on the device identified by the <MAC/HOSTNAME> keyword • <MAC/HOSTNAME> – Specify the device's MAC address or hostname.

no-reboot {staggered-reboot}	Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)
reboot-time <TIME> {staggered-reboot}	Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.
staggered-reboot	This keyword is common to all of the above. • Optional. Enables staggered reboot (one at a time), without network impact

`device-upgrade rf-domain [<RF-DOMAIN-NAME>|all] [all|br650|br6511|br1220|br71xx|br81xx|rfs4000|rfs6000|rfs7000] {from-controller {no-reboot|reboot-time <TIME>|upgrade-time <TIME> {no-reboot|reboot-time <TIME>}} {(staggered-reboot)}`

rf-domain [<RF-DOMAIN-NAME>|all]	Upgrades firmware on devices in a specified RF Domain or all RF Domains • <RF-DOMAIN-NAME> – Upgrades devices in a specified RF Domain. Specify the RF Domain name. • all – Upgrades devices across all RF Domains
[all|br650|br6511|br1220|br71xx|br81xx|rfs4000|rfs6000|rfs7000]	After specifying the RF Domain, select the device type. • all – Upgrades firmware on all devices • Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point • Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000 • Service Platforms — Brocade Mobility RFS9510 • Brocade Mobility 650 Access Point – Upgrades firmware on all Brocade Mobility 650 Access Points • Brocade Mobility 6511 Access Point – Upgrades firmware on all Brocade Mobility 6511 Access Points • Brocade Mobility 1220 Access Point – Upgrades firmware on all Brocade Mobility 1220 Access Points • Brocade Mobility 71XX Access Point – Upgrades firmware on all Brocade Mobility 71XX Access Points • Brocade Mobility 1240 Access Point – Upgrades firmware on all Brocade Mobility 1240 Access Points • Brocade Mobility RFS4000 – Upgrades firmware on all Brocade Mobility RFS4000s • Brocade Mobility RFS6000 – Upgrades firmware on all Brocade Mobility RFS6000s • Brocade Mobility RFS7000 – Upgrades firmware on all Brocade Mobility RFS7000s
from-controller	Optional. Upgrades a device through the adopted device
no-reboot {staggered-reboot}	Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)
reboot-time <TIME> {staggered-reboot}	Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.
upgrade-time <TIME> {no-reboot|reboot-time <TIME>}	Optional. Schedules an automatic firmware upgrade • <TIME> – Specify the upgrade time in the MM/DD/YYYY-HH:MM or HH:MM format. After a scheduled upgrade, the following actions can be performed: • no-reboot – Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted) • reboot-time <TIME> – Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.
staggered-reboot	This keyword is common to all of the above. • Optional. Enables staggered reboot (one at a time), without network impact

```
device-upgrade rf-domain [<RF-DOMAIN-NAME>|all]
[all|br650|br6511|br1220|br71xx|br81xx|rfs4000|rfs6000|rfs7000] {upgrade-time
<TIME> {no-reboot|reboot-time <TIME>}} {(staggered-reboot)}
```

rf-domain [<RF-DOMAIN-NAME>| all]	Upgrades firmware on devices in a specified RF Domain or all RF Domains • <RF-DOMAIN-NAME> – Upgrades devices in a specified RF Domain. Specify the RF Domain name. • all – Upgrades devices across all RF Domains
[all|br650|br6511|br1220|br71xx|br81xx|rfs4000|rfs6000|rfs7000]	After specifying the RF Domain, select the device type. • all – Upgrades firmware on all devices • Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point • Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000 • Service Platforms — Brocade Mobility RFS9510 • Brocade Mobility 650 Access Point – Upgrades firmware on all Brocade Mobility 650 Access Points • Brocade Mobility 6511 Access Point – Upgrades firmware on all Brocade Mobility 6511 Access Points • Brocade Mobility 1220 Access Point – Upgrades firmware on all Brocade Mobility 1220 Access Points • Brocade Mobility 71XX Access Point – Upgrades firmware on all Brocade Mobility 71XX Access Points • Brocade Mobility 1240 Access Point – Upgrades firmware on all Brocade Mobility 1240 Access Points • Brocade Mobility RFS4000 – Upgrades firmware on all Brocade Mobility RFS4000s • Brocade Mobility RFS6000 – Upgrades firmware on all Brocade Mobility RFS6000s • Brocade Mobility RFS7000 – Upgrades firmware on all Brocade Mobility RFS7000s
upgrade <TIME>	Optional. Schedules an automatic device firmware upgrade • <TIME> – Specify the upgrade time in the MM/DD/YYYY-HH:MM or HH:MM format.
no-reboot {staggered-reboot}	Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)
reboot-time <TIME> {staggered-reboot}	Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.
staggered-reboot	This keyword is common to all of the above. • Optional. Enables staggered reboot (one at a time), without network impact

Usage Guidelines: (NOC controller adoption matrix)

The following table displays NOC controllers and the corresponding site-level controllers supported by each:

Site Controllers supported by each NOC controller	NOC Controllers
	Brocade Mobility RFS7000
Brocade Mobility RFS4000	X
Brocade Mobility RFS6000	X
Brocade Mobility RFS7000	X

Example

```
rfs4000-229D58#device-upgrade rfs4000-229D58 no-reboot
rfs4000-229D58#

rfs4000-229D58#show device-upgrade ?
  history           History of Device Upgrade
  load-image-status  Status of firmware file download on the device
```

```
  status             Status of Device Upgrade
  versions           Versions of device-upgrade images

rfs4000-229D58#show device-upgrade

rfs4000-229D58#show device-upgrade history
--------------------------------------------------------------------------------
--------------------
           Device      RESULT                TIME  RETRIES       UPGRADED-BY
LAST-UPDATE-ERROR
--------------------------------------------------------------------------------
--------------------

     br71xx-0F43D8     failed  2013-01-05 00:21:08       3  00-23-68-22-9D-58
Update error:  Unable to get update file, failure in ftp/openssl/tar

     ap6532-986C50     failed  2013-01-05 00:26:31       3  00-23-68-22-9D-58
Update error:  Bad file, failure in tar. tar: invalid tar magic
Total number of entries displayed: 2
rfs4000-229D58#

rfs4000-229D58#show device-upgrade versions
--------------------------------------------------------------------------------
---
          CONTROLLER              DEVICE-TYPE                  VERSION
--------------------------------------------------------------------------------
---
rfs4000-229D58              br650                 5.5.0.0-023D
rfs4000-229D58              br6511                none
rfs4000-229D58              br1220                5.5.0.0-023D
rfs4000-229D58              br71xx                none
rfs4000-229D58              br81xx                none
rfs4000-229D58              rfs4000               none
--------------------------------------------------------------------------------
---
rfs4000-229D58#
```

diff

Privileged Exec Mode Commands

Displays the differences between two files on a device's file system or a particular URL

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — , Brocade Mobility RFS9510

Syntax:

```
diff [<FILE>|<URL>] [<FILE>|<URL>]
```

Parameters

```
diff [<FILE>|<URL>] [<FILE>|<URL>]
```

<FILE>	The first <FILE> is the source file for the diff command. The second <FILE> is used for comparison.
<URL>	The first <URL> is the source file's URL. The second <URL> is the second file's URL.

Example

```
rfs4000-229D58#diff startup-config running-config
--- startup-config
+++ running-config
@@ -1,3 +1,4 @@
+!### show running-config
 !
 ! Configuration of Brocade Mobility RFS4000 version 5.5.0.0-015D
 !
@@ -495,13 +496,11 @@
  service-alias testing index 10 proto 9 destination-port range 21 21
 !
 rfs4000 00-23-68-22-9D-58
- radio-count 0
  use profile default-rfs4000
  use rf-domain default
  hostname rfs4000-229D58
  license AP DEFAULT-6AP-LICENSE
  license ADSEC DEFAULT-ADV-SEC-LICENSE
- no adoption-site
  ip default-gateway 192.168.13.2
  ip default-gateway priority static-route 20
  interface ge1
rfs4000-229D58#
```

dir

Privileged Exec Mode Commands

Lists files on a device's file system

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
dir {/all|/recursive|<DIR>|all-filesystems}
```

Parameters

```
dir {/all|/recursive|<DIR>|all-filesystems}
```

/all	Optional. Lists all files
/recursive	Optional. Lists files recursively

<DIR>	Optional. Lists files in the named file path
all-filesystems	Optional. Lists files on all file systems

Example

```
rfs4000-229D58#dir
Directory of flash:/.

  drwx             Wed Jan 30 02:45:10 2013   log
  drwx             Sat Jan  1 00:00:09 2000   configs
  drwx             Sat Jan  1 00:00:08 2000   cache
  drwx             Wed Jan 16 22:26:53 2013   crashinfo
  drwx             Wed Jan 16 22:57:14 2013   archived_logs
  drwx             Sat Jan  1 00:00:08 2000   upgrade
  drwx             Sat Jan  1 00:00:09 2000   hotspot
  drwx             Sat Jan  1 00:00:09 2000   floorplans
  drwx             Sat Jan  1 00:00:09 2000   startuplog
  -rw-   176128    Fri Feb 15 14:32:51 2013   out.tar

rfs4000-229D58#

rfs4000-229D58#dir all-filesystems
Directory of flash:/

  drwx             Wed Jan 30 02:45:10 2013   log
  drwx             Sat Jan  1 00:00:09 2000   configs
  drwx             Sat Jan  1 00:00:08 2000   cache
  drwx             Wed Jan 16 22:26:53 2013   crashinfo
  drwx             Wed Jan 16 22:57:14 2013   archived_logs
  drwx             Sat Jan  1 00:00:08 2000   upgrade
  drwx             Sat Jan  1 00:00:09 2000   hotspot
  drwx             Sat Jan  1 00:00:09 2000   floorplans
  drwx             Sat Jan  1 00:00:09 2000   startuplog
  -rw-   176128    Fri Feb 15 14:32:51 2013   out.tar

Directory of nvram:/

  -rw-   10669     Sat Jan 14 02:47:11 2012   startup-config.save
  -rw-   69        Wed Jan 16 22:37:59 2013   licenses
  -rw-   14785     Wed Jan 16 22:37:07 2013   startup-config

Directory of system:/

  drwx             Wed Jan 16 22:35:18 2013   proc

rfs4000-229D58#
```

disable

Privileged Exec Mode Commands

Turns off (disables) the privileged mode command set. This command returns to the User Executable mode.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
disable
```

Parameters

None

Example

```
rfs7000-37FABE#disable
rfs7000-37FABE>
```

edit

Privileged Exec Mode Commands

Edits a text file on the device's file system

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
edit <FILE>
```

Parameters

```
edit <FILE>
```

<FILE>	Specify the name of the file to modify.

Example

```
rfs4000-229D58#edit startup-config
  GNU nano 1.2.4               File: startup-config

!
! Configuration of Brocade Mobility RFS4000 version 5.5.0.0-034B
!
!
version 2.3
!
!
client-identity TestClientIdentity
```

```
 dhcp 1 message-type request option-codes exact hexstring 5e4d36780b3a7f
!
client-identity-group ClientIdentityGroup
 client-identity TestClientIdentity precedence 1
!
ip access-list BROADCAST-MULTICAST-CONTROL
 permit tcp any any rule-precedence 10 rule-description "permit all TCP
traffic"
 permit udp any eq 67 any eq dhcpc rule-precedence 11 rule-description "permit
$
 deny udp any range 137 138 any range 137 138 rule-precedence 20
rule-descripti$
 deny ip any 224.0.0.0/4 rule-precedence 21 rule-description "deny IP
multicast"
 deny ip any host 255.255.255.255 rule-precedence 22 rule-description "deny IP
$
                                [ Read 549 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Txt ^T To Spell
```

enable

Privileged Exec Mode Commands

Turns on (enables) the privileged mode command set. This command does not do anything in the Privilege Executable mode.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
enable
```

Parameters

None

Example

```
rfs7000-37FABE#enable
rfs7000-37FABE#
```

erase

Privileged Exec Mode Commands

Erases a device's (wireless controller, access point, and service platform) file system. Erases the content of the specified storage device. Also erases the startup configuration to restore the device to its default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
erase [cf:|flash:|nvram:|startup-config|usb1:]
```

Parameters

```
erase [cf:|flash:|nvram:|startup-config|usb1:]
```

cf:	Erases everything in the device's cf: file
flash:	Erases everything in the device's flash: file
nvram:	Erases everything in the device's nvram: file
startup-config	Erases the device's startup configuration file. The startup configuration file is used to configure the device when it reboots.
usb1:	Erases everything in the device's usb1: file

Example

```
rfs7000-37FABE#erase startup-config
Erase startup-config? (y/n): n
rfs7000-37FABE#
```

halt

Privileged Exec Mode Commands

Stops (halts) a device (access point, wireless controller, or service platform). Once halted, the system must be restarted manually.

This command stops the device immediately. No indications or notifications are provided while the device shuts down.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
halt {on <DEVICE-NAME>}
```

Parameters

```
halt {on <DEVICE-NAME>}
```

halt {on <DEVICE-NAME>}	Halts a specified device • on <DEVICE-NAME> – Optional. Enter the name of the AP, wireless controller, or service platform. If the device name is not specified, the logged device is halted.

Example

```
rfs7000-37FABE#halt on rfs7000-37FABE
rfs7000-37FABE#
```

join-cluster

Privileged Exec Mode Commands

Adds a device (access point, wireless controller, or service platform), as cluster member, to an existing cluster of devices. Assign a static IP address to the device before adding to a cluster.

Supported in the following platforms:

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
join-cluster <IP> user <USERNAME> password <WORD> {level|mode}
join-cluster <IP> user <USERNAME> password <WORD> {level [1|2]|mode
[active|standby]}
```

Parameters

```
join-cluster <IP> user <USERNAME> password <WORD> {level [1|2]|mode
[active|standby]}
```

join-cluster	Adds a access point, wireless controller, or service platform to an existing cluster
<IP>	Specify the cluster member's IP address.
user <USERNAME>	Specify a user account with super user privileges on the new cluster member.
password <WORD>	Specify password for the account specified in the user parameter.
level [1|2]	Optional. Configures the routing level • 1 – Configures level 1 routing • 2 – Configures level 2 routing
mode [active|standby]	Optional. Configures the cluster mode • active – Configures cluster mode as active • standby – Configures cluster mode as standby

Usage Guidelines:

To add a device to an existing cluster:

- Configure a static IP address on the device (access point, wireless controller, or service platform).
- Provide username and password for superuser, network admin, system admin, or operator accounts.

After adding the device to a cluster, execute the “write memory” command to ensure the configuration persists across reboots.

Example

```
rfs7000-37FABE#join-cluster 172.16.10.10 user admin password admin123
Joining cluster at 172.16.10.10... Done
Please execute “write memory” to save cluster configuration.
rfs7000-37FABE#

nx6500-31FABE#join-cluster 172.16.10.10 user admin password admin123
Joining cluster at 172.16.10.10... Done
Please execute “write memory” to save cluster configuration.
nx6500-31FABE#
```

Related Commands:

cluster	Initiates the cluster context. The cluster context provides centralized management to configure all cluster members from any one member.
create-cluster	Creates a new cluster on a specified device

l2tpv3

Privileged Exec Mode Commands

Establishes or brings down an L2TPv3 tunnel

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
l2tpv3 tunnel [<TUNNEL-NAME>|all]

l2tpv3 tunnel <TUNNEL-NAME> [down|session|up]
l2tpv3 tunnel <TUNNEL-NAME> [down|up] {on <DEVICE-NAME>}
l2tpv3 tunnel <TUNNEL-NAME> session <SESSION-NAME> [down|up] {on
<DEVICE-NAME>}

l2tpv3 tunnel all [down|up] {on <DEVICE-NAME>}
```

Parameters

```
l2tpv3 tunnel <TUNNEL-NAME> [down|up] {on <DEVICE-NAME>}
```

l2tpv3 tunnel <TUNNEL-NAME> [down|up]	Establishes or brings down an L2TPv3 tunnel • <TUNNEL-NAME> – Specify the tunnel name. • down – Brings down the specified tunnel • up – Establishes the specified tunnel
on <DEVICE-NAME>	Optional. Establishes or brings down a tunnel on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
l2tpv3 tunnel <TUNNEL-NAME> session <SESSION-NAME> [down|up] {on
<DEVICE-NAME>}
```

l2tpv3 tunnel <TUNNEL-NAME>	Establishes or brings down an L2TPv3 tunnel • <TUNNEL-NAME> – Specify the tunnel name.
session <SESSION-NAME> [down|up]	Establishes or brings down a session in the specified tunnel • <SESSION-NAME> – Specify the session name. • down – Brings down the specified tunnel session • up – Establishes the specified tunnel session
on <DEVICE-NAME>	Optional. Establishes or brings down a tunnel session on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
l2tpv3 tunnel all [down|up] {on <DEVICE-NAME>}
```

l2tpv3 tunnel	Establishes or brings down a L2TPv3 tunnel
all [down|up]	Establishes or brings down all L2TPv3 tunnels • down – Brings down all tunnels • up – Establishes all tunnels
on <DEVICE-NAME>	Optional. Establishes or brings down all tunnels on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Example

```
rfs7000-37FABE#l2tpv3 tunnel Tunnel1 session Tunnel1Session1 up on
rfs7000-37FABE
```

NOTE
For more information on the L2TPv3 tunnel configuration mode and commands, see *Chapter 23, L2TPV3-POLICY*.

logging

Privileged Exec Mode Commands

Modifies message logging settings

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
logging monitor
{<0-7>|alerts|critical|debugging|emergencies|errors|informational|
          warnings|notifications}
```

Parameters

```
logging monitor
{<0-7>|alerts|critical|debugging|emergencies|errors|informational|
notifications|warnings}
```

monitor	Sets terminal lines logging levels. The logging severity levels can be set from 0 - 7. The system configures default settings, if no logging severity level is specified. • <0-7> – Optional. Enter the logging severity level from 0 - 7. The various levels and their implications are: • alerts – Optional. Immediate action needed (severity=1) • critical – Optional. Critical conditions (severity=2) • debugging – Optional. Debugging messages (severity=7) • emergencies – Optional. System is unusable (severity=0) • errors – Optional. Error conditions (severity=3) • informational – Optional. Informational messages (severity=6) • notifications – Optional. Normal but significant conditions (severity=5) • warnings – Optional. Warning conditions (severity=4)

Example

```
rfs7000-37FABE#logging monitor warnings
rfs7000-37FABE#

rfs7000-37FABE#logging monitor 2
rfs7000-37FABE#
```

Related Commands:

no	Resets terminal lines logging levels

mint

Privileged Exec Mode Commands

Uses MiNT protocol to perform a ping and traceroute to a remote device

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
mint [ping|traceroute]

mint ping <MINT-ID> {count <1-10000>|size <1-64000>|timeout <1-10>}

mint traceroute <MINT-ID> {destination-port <1-65535>|max-hops <1-255>|
          source-port <1-65535>|timeout <1-255>}
```

Parameters

```
mint ping MINT-ID {count <1-10000>|size <1-64000>|timeout <1-10>}
```

ping <MINT-ID>	Sends a MiNT echo message to a specified destination • <MINT-ID> – Specify the destination device's MiNT ID.
count <1-10000>	Optional. Sets the pings to the MiNT destination • <1-10000> – Specify a value from 1 - 60. The default is 3.
size <1-64000>	Optional. Sets the MiNT payload size in bytes • <1-64000> – Specify a value from 1 - 640000 bytes. The default is 64 bytes.
timeout <1-10>	Optional. Sets a response time in seconds • <1-10> – Specify a value from 1 - 10 seconds. The default is 1 second.

```
mint traceroute MINT-ID {destination-port <1-65535>|max-hops <1-255>|
source-port <1-65535>|timeout <1-255>}
```

traceroute <MINT-ID>	Prints the route packets trace to a device • <MINT-ID> – Specify the destination device's MiNT ID.
destination-port <1-65535>	Optional. Sets the *Equal-cost Multi-path* (ECMP) routing destination port • <1-65535> – Specify a value from 1 - 65535. The default port is 45.
max-hops <1-255>	Optional. Sets the maximum number of hops a traceroute packet traverses in the forward direction • <1-255> – Specify a value from 1 - 255. The default is 30.
source-port <1-65535>	Optional.Sets the ECMP source port • <1-65535> – Specify a value from 1 - 65535. The default port is 45.
timeout <1-255>	Optional. Sets the minimum response time period • <1-65535> – Specify a value from 1 - 255 seconds. The default is 30 seconds.

Example

```
rfs7000-37FABE#mint ping 70.37.FA.BF count 20 size 128
MiNT ping 70.37.FA.BF with 128 bytes of data.
 Response from 70.37.FA.BF: id=1 time=0.292 ms
 Response from 70.37.FA.BF: id=2 time=0.206 ms
 Response from 70.37.FA.BF: id=3 time=0.184 ms
 Response from 70.37.FA.BF: id=4 time=0.160 ms
 Response from 70.37.FA.BF: id=5 time=0.138 ms
 Response from 70.37.FA.BF: id=6 time=0.161 ms
 Response from 70.37.FA.BF: id=7 time=0.174 ms
 Response from 70.37.FA.BF: id=8 time=0.207 ms
 Response from 70.37.FA.BF: id=9 time=0.157 ms
 Response from 70.37.FA.BF: id=10 time=0.153 ms
 Response from 70.37.FA.BF: id=11 time=0.159 ms
 Response from 70.37.FA.BF: id=12 time=0.173 ms
 Response from 70.37.FA.BF: id=13 time=0.156 ms
 Response from 70.37.FA.BF: id=14 time=0.209 ms
 Response from 70.37.FA.BF: id=15 time=0.147 ms
 Response from 70.37.FA.BF: id=16 time=0.203 ms
 Response from 70.37.FA.BF: id=17 time=0.148 ms
 Response from 70.37.FA.BF: id=18 time=0.169 ms
 Response from 70.37.FA.BF: id=19 time=0.164 ms
 Response from 70.37.FA.BF: id=20 time=0.177 ms

--- 70.37.FA.BF ping statistics ---
20 packets transmitted, 20 packets received, 0% packet loss
round-trip min/avg/max = 0.138/0.177/0.292 ms
rfs7000-37FABE#
```

mkdir

Privileged Exec Mode Commands

Creates a new directory in the file system

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
mkdir <DIR>
```

Parameters

```
mkdir <DIR>
```

<DIR>	Specify a directory name. **NOTE:** A directory, specified by the <DIR> parameter, is created within the file system.

Example

```
rfs4000-229D58#dir
Directory of flash:/.

  drwx             Wed Jan 30 02:45:10 2013   log
  drwx             Sat Jan  1 00:00:09 2000   configs
  drwx             Sat Jan  1 00:00:08 2000   cache
  drwx             Wed Jan 16 22:26:53 2013   crashinfo
  drwx             Wed Jan 16 22:57:14 2013   archived_logs
  drwx             Sat Jan  1 00:00:08 2000   upgrade
  drwx             Sat Jan  1 00:00:09 2000   hotspot
  drwx             Sat Jan  1 00:00:09 2000   floorplans
  drwx             Sat Jan  1 00:00:09 2000   startuplog
  -rw-   176128    Fri Feb 15 14:32:51 2013   out.tar

rfs4000-229D58#

rfs4000-229D58#mkdir testdir
rfs4000-229D58#

rfs4000-229D58#dir
Directory of flash:/.

  drwx             Wed Jan 30 02:45:10 2013   log
  drwx             Sat Jan  1 00:00:09 2000   configs
  drwx             Sat Jan  1 00:00:08 2000   cache
  drwx             Wed Jan 16 22:26:53 2013   crashinfo
  drwx             Fri Feb 15 14:50:49 2013   testdir
  drwx             Wed Jan 16 22:57:14 2013   archived_logs
  drwx             Sat Jan  1 00:00:08 2000   upgrade
  drwx             Sat Jan  1 00:00:09 2000   hotspot
  drwx             Sat Jan  1 00:00:09 2000   floorplans
```

```
  drwx             Sat Jan  1 00:00:09 2000   startuplog
  -rw-   176128    Fri Feb 15 14:32:51 2013   out.tar

rfs4000-229D58#
```

more

Privileged Exec Mode Commands

Displays files on the device's file system. This command navigates and displays specific files in the device's file system. Provide the complete path to the file `more <file>`.

The more command also displays the startup configuration file.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
more <FILE>
```

Parameters

```
more <FILE>
```

<FILE>	Specify the file name and location.

Example

```
rfs4000-229D58#more flash:/log/messages.log
Jan 01 00:04:12 2013: rfs4000-229D58 : %SYSTEM-3-LOGIN_FAIL: Log-in failed for
user 'admin' from 'ssh'
Jan 01 02:06:53 2013: rfs4000-229D58 : %SYSTEM-3-LOGIN_FAIL: Log-in failed for
user 'admin'superuser' from 'ssh'
Jan 01 02:07:01 2013: rfs4000-229D58 : %SYSTEM-3-LOGIN_FAIL: Log-in failed for
user 'admin'superuser' from 'ssh'
Jan 01 02:23:26 2013: rfs4000-229D58 : %NSM-4-IFDOWN: Interface ge1 is down
Jan 01 02:24:25 2013: rfs4000-229D58 : %NSM-4-IFUP: Interface ge1 is up
Jan 01 02:24:26 2013: rfs4000-229D58 : %NSM-4-IFUP: Interface ge1 is up
Jan 01 02:24:33 2013: rfs4000-229D58 : %NSM-4-IFDOWN: Interface ge1 is down
Jan 01 02:24:40 2013: rfs4000-229D58 : %NSM-4-IFUP: Interface ge1 is up
Jan 01 02:24:40 2013: rfs4000-229D58 : %NSM-4-IFUP: Interface ge1 is up
rfs4000-229D58#
```

no

Privileged Exec Mode Commands

Use the no command to revert a command or a set of parameters to their default. This command is useful to turn off an enabled feature or to revert to default settings.

The no commands have their own set of parameters that can be reset. These parameters depend on the context in which the command is being used.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no
[adoption|captive-portal|crypto|debug|logging|mac-user-db|page|raid|service|
          terminal|upgrade|virtual-machine|wireless]

no adoption {on <DEVICE-OR-DOMAIN-NAME>}

no captive-portal client [captive-portal <CAPTIVE-PORTAL-NAME>|mac <MAC>]
          {on <DEVICE-OR-DOMAIN-NAME>}

no crypto pki [server|trustpoint]
no crypto pki [server|trustpoint] <TRUSTPOINT-NAME> {del-key {on
<DEVICE-NAME>}|
  on <DEVICE-NAME>}

no logging monitor

no page

no service [block-adopter-config-update|locator|ssm|wireless]
no service block-adopter-config-update
no service locator {on <DEVICE-NAME>}
no service [ssm|wireless] trace pattern {<WORD>|on <DEVICE-NAME>}

no terminal [length|width]

no upgrade <PATCH-NAME> {on <DEVICE-NAME>}

no wireless client [all|<MAC>]
no wireless client all {filter|on}
no wireless client all {filter [wlan <WLAN-NAME>]}
no wireless client all {on <DEVICE-OR-DOMAIN-NAME>} {filter [wlan
<WLAN-NAME>]}
no wireless client mac <MAC> {on <DEVICE-OR-DOMAIN-NAME>}
```

Parameters

```
no adoption {on <DEVICE-OR-DOMAIN-NAME>}
```

no adoption {on <DEVICE-OR-DOMAIN-NAME>}	Resets adoption status of a specified device or all devices in a specified RF Domain • <DEVICE-OR-DOMAIN-NAME> – Optional. Enter the name of the AP, wireless controller, service platform, or RF Domain. This command resets the adoption status of the specified device and all devices adopted by it.

`no captive-portal client [captive-portal <CAPTIVE-PORTAL-NAME>|<MAC>] {on <DEVICE-OR-DOMAIN-NAME>}`

no captive-portal client	Disconnects captive portal clients from the network
captive-portal <CAPTIVE-PORTAL-NAME>	Disconnects captive portal clients • <CAPTIVE-PORTAL-NAME> – Specify the captive portal name.
<MAC>	Disconnects a specified client • <MAC> – Specify the client's MAC address.
on <DEVICE-OR-DOMAIN-NAME>	Optional. Disconnects a specified captive portal client or all clients on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

`no crypto pki [server|trustpoint] <TRUSTPOINT-NAME> {del-key {on <DEVICE-NAME>}| on <DEVICE-NAME>}`

no crypto pki	Deletes all PKI authentications
[server|trustpoint] <TRUSTPOINT-NAME>	Deletes PKI authentications, such as server certificates and trustpoints • server – Deletes server certificates • trustpoint – Deletes a trustpoint and its associated certificates The following keyword is common to the server and trustpoint parameters: • <TURSTPOINT-NAME> – Deletes a trustpoint or its server certificate. Specify the trustpoint name.
del-key {on <DEVICE-NAME>}	Optional. Deletes the private key associated with a server certificate or trustpoint. The operation fails if the private key is in use by other trustpoints. • on <DEVICE-NAME> – Deletes the private key on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`no logging monitor`

no logging monitor	Resets terminal lines message logging levels

`no page`

no page	Resets controller paging function to its default. Disabling the "page" command displays the CLI command output at once, instead of page by page.

`no service block-adopter-config-update`

no service	Disables certain specified services or features
block-adopter-config-update	Enables configuration updates from the NOC controller. If the configuration update from the NOC controller feature is blocked, use the *no* > *service* > *block-adopter-config-update* command to enable it.

`no service locator {on <DEVICE-NAME>}`

no service	Disables LEDs on a specified device in the WLAN. It also resets the CLI table expand and MiNT protocol configurations.
locator {on <DEVICE-NAME>}	Disables LEDs on a specified device • <DEVICE-NAME> – Optional. Specify the name of the AP, wireless controller, or service platform.

`no service [ssm|wireless] trace pattern {<WORD>|on <DEVICE-NAME>}`

no service	Disables certain specified services or features
[ssm|traceroute]	Disables the following features: • ssm – Disables *Security Services Module* (SSM) related services • traceroute – Disables wireless related services

trace	The following command is common to the 'ssm' and 'wireless' parameters: • trace – Traces SSM or wireless related services
pattern {<WORD>| on <DEVICE-NAME>}	Configures the pattern to match • <WORD> – Optional. Specify the pattern to ignore. Reverses the match pattern specified. • on <DEVICE-NAME> – Optional. Matches the specified pattern on specified device. • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`no upgrade <PATCH-NAME> {on <DEVICE-NAME>}`

no upgrade <PATCH-NAME>	Removes a patch installed on a specified device • <PATCH-NAME> – Specify the name of the patch.
on <DEVICE-NAME>	Optional. Removes a patch on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`no terminal [length|width]`

no terminal [length|width]	Resets the width of the terminal window, or the number of lines displayed within the terminal window • length – Resets the number of lines displayed on the terminal window to its default • width – Resets the width of the terminal window to its default.

`no wireless client all {filter [wlan <WLAN-NAME>]}`

no wireless client all	Disassociates all wireless clients on a specified device or domain
filter wlan <WLAN-NAME>	Optional. Specifies an additional client selection filter • wlan – Filters clients on a specified WLAN • <WLAN-NAME> – Specify the WLAN name.

`no wireless client all {on <DEVICE-OR-DOMAIN-NAME>} {filter [wlan <WLAN-NAME>]}`

no wireless client all on <DEVICE-OR-DOMAIN-NAME>	Disassociates all clients on a specified device or domain • <DEVICE-OR-DOMAIN-NAME> – Optional. Specify the name of the AP, wireless controller, service platform, or RF Domain.
filter [wlan <WLAN-NAME>]	Optional. Specifies an additional client selection filter • wlan – Filters clients on a specified WLAN • <WLAN-NAME> – Specify the WLAN name.

`no wireless client mac <MAC> {on <DEVICE-OR-DOMAIN-NAME>}`

no wireless client mac <MAC>	Disassociates a single wireless client on a specified device or RF Domain • mac <MAC> – Specify the wireless client's MAC address in the AA-BB-CC-DD-EE-FF format
on <DEVICE-OR-DOMAIN-NAME >	Optional. Specifies the name of the AP, wireless controller, service platform, or RF Domain to which the specified client is associated

`no virtual-machine assign-usb-ports {on <DEVICE-NAME>}`

no virtual-machine assign-usb-ports	Reverts ports assigned for virtual-machines back to Mobility This command is available only on the Brocade Mobility RFS9510 series service platforms.
on <DEVICE-NAME>	Reverts virtual-machine assigned ports on a specified device • on <DEVICE-NAME> – Optional. Specify the name of the AP, wireless controller, or service platform.

	`no mac-user-db user [<USER-NAME>|all]`
no mac-user-db user	Deletes a specified user or all users from the MAC registration user database This command is available only on the NX9000 series service platforms.
<USER-NAME>	Deletes the user, identified by the <USER-NAME> keyword, from the MAC registration user database • <USER-NAME> – Specify the username.
all	Deletes all users from the MAC registration user database

	`no raid locate`
no raid locate	Disables flashing of LEDs on RAID drives. This command is available only on the NX9000 series service platforms For more information on RAIDs and enabling LEDs on RAID drives, see *raid*.

Usage Guidelines:

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
rfs7000-37FABE#no adoption
rfs7000-37FABE#

rfs7000-37FABE#no page
rfs7000-37FABE#

rfs7000-37FABE#no service cli-tables-expand line
rfs7000-37FABE#
```

Related Commands:

auto-provisioning-policy	Resets the adoption state of a device and all devices adopted to it
captive portal	Manages captive portal clients
crypto	Enables digital certificate configuration and RSA Keypair management
logging	Modifies message logging settings
page	Resets controller paging function to its default
service	Performs different functions depending on the parameter passed
terminal	Sets the length or the number of lines displayed within the terminal window
upgrade	Upgrades software image on a device
wireless-client	Manages wireless clients
virtual-machine	Installs, configures, and monitors the status of third-party VMs
raid	Enables *Redundant Array of Independent Disks* (RAID) management

page

Privileged Exec Mode Commands

Toggles controller paging. Enabling this command displays the CLI command output page by page, instead of running the entire output at once.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
page
```

Parameters

None

Example

```
rfs7000-37FABE#page
rfs7000-37FABE#
```

Related Commands:

no	Disables controller paging

ping

Privileged Exec Mode Commands

Sends *Internet Controller Message Protocol* (ICMP) echo messages to a user-specified location

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
ping <IP/HOSTNAME> {count <1-10000>|dont-fragment {count|size}|size <1-64000>}
```

Parameters

```
ping <IP/HOSTNAME> {count <1-10000>|dont-fragment {count|size}|size <1-64000>}
```

<IP/HOSTNAME>	Specify the destination IP address or hostname to ping. When entered without any parameters, this command prompts for an IP address or a hostname.
count <1-10000>	Optional. Sets the pings to the specified destination • <1-10000> – Specify a value from 1 - 10000. The default is 5.

dont-fragment {count|size}	Optional. Sets the dont-fragment bit in the ping packet. Packets with the dont-fragment bit specified, are not fragmented. When a packet, with the dont-fragment bit specified, exceeds the specified *Maximum Transmission Unit* (MTU) value, an error message is sent from the device trying to fragment it. • count <1-10000> – Sets the pings to the specified destination from 1 - 10000. The default is 5. • size – <1-64000> – Sets the size of ping payload size from 1 - 64000 bytes. The default is 100 bytes.
size <1-64000>	Optional. Sets the ping packet's size in bytes • <1-64000> – Specify the ping payload size from 1 - 64000 bytes. The default is 100 bytes.

Example

```
rfs7000-37FABE#ping 172.16.10.4 count 6
PING 172.16.10.4 (172.16.10.4) 100(128) bytes of data.
108 bytes from 172.16.10.4: icmp_seq=1 ttl=64 time=3.93 ms
108 bytes from 172.16.10.4: icmp_seq=2 ttl=64 time=0.367 ms
108 bytes from 172.16.10.4: icmp_seq=3 ttl=64 time=0.328 ms
108 bytes from 172.16.10.4: icmp_seq=4 ttl=64 time=0.295 ms
108 bytes from 172.16.10.4: icmp_seq=5 ttl=64 time=0.340 ms
108 bytes from 172.16.10.4: icmp_seq=6 ttl=64 time=0.371 ms

--- 172.16.10.4 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5001ms
rtt min/avg/max/mdev = 0.295/0.939/3.936/1.340 ms
rfs7000-37FABE#
```

pwd

Privileged Exec Mode Commands

Displays the full path of the present working directory, similar to the UNIX pwd command

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
pwd
```

Parameters

None

Example

```
rfs4000-229D58#pwd
flash:/
rfs4000-229D58#

rfs4000-229D58#dir
Directory of flash:/.

  drwx            Wed Jan 30 02:45:10 2013   log
  drwx            Sat Jan  1 00:00:09 2000   configs
```

```
  drwx             Sat Jan  1 00:00:08 2000   cache
  drwx             Wed Jan 16 22:26:53 2013   crashinfo
  drwx             Fri Feb 15 14:50:49 2013   testdir
  drwx             Wed Jan 16 22:57:14 2013   archived_logs
  drwx             Sat Jan  1 00:00:08 2000   upgrade
  drwx             Sat Jan  1 00:00:09 2000   hotspot
  drwx             Sat Jan  1 00:00:09 2000   floorplans
  drwx             Sat Jan  1 00:00:09 2000   startuplog
  -rw-   176128    Fri Feb 15 14:32:51 2013   out.tar

rfs4000-229D58#
```

re-elect

Privileged Exec Mode Commands

Re-elects the tunnel controller (wireless controller or service platform)

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
re-elect tunnel-controller {<WORD> {on <DEVICE-NAME>}|on <DEVICE-NAME>}
```

Parameters

```
re-elect tunnel-controller {<WORD> {on <DEVICE-NAME>}|on <DEVICE-NAME>}
```

re-elect tunnel-controller	Re-elects the tunnel controller
<WORD> {on <DEVICE-NAME>}	Optional. Re-elects the tunnel controller on all devices whose preferred tunnel controller name matches <WORD> • on <DEVICE-NAME> – Optional. Re-elects the tunnel controller on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Example

```
rfs7000-37FABE#re-elect tunnel-controller
OK
rfs7000-37FABE#
```

reload

Privileged Exec Mode Commands

Halts the device and performs a warm reboot

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
reload {cancel|force|in|on}
reload {on <DEVICE-OR-DOMAIN-NAME>}
reload {cancel|force} {on <DEVICE-OR-DOMAIN-NAME>}
reload {in <1-999>} {list|on}
reload {in <1-999>} {list {<LINE>|all}|on <DEVICE-OR-DOMAIN-NAME>}
reload {in <1-999>} {on <DEVICE-OR-DOMAIN-NAME>}
```

Parameters

`reload {on <DEVICE-OR-DOMAIN-NAME>}`

on <DEVICE-OR-DOMIN-NAME>	Optional. Performs reload on a specified device or RF Domain. Halts the system and performs a warm reboot • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

`reload {cancel|force} {on <DEVICE-OR-DOMAIN-NAME>}`

cancel	Optional. Cancels pending reloads
force	Optional. Forces reboot, while ignoring conditions like upgrade in progress, unsaved changes etc.
on <DEVICE-OR-DOMAIN-NAME>	Optional. Cancels or forces a reload on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

`reload {in <1-999>} {list {<LINE>|all}|on <DEVICE-OR-DOMAIN-NAME>}`

in <1-999>	Optional. Performs a reload after a specified time period • <1-999> – Specify the time from 1 - 999 minutes.
list {<LINE>|all}	Optional. Reloads all adopted devices or specified devices • <LINE> – Optional. Reloads listed devices. List all devices (to be reloaded) separated by a space • all – Optional. Reloads all devices adopted by this controller
on <DEVICE-OR-DOMAIN-NAME>	Optional. Reloads on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

Example

```
rfs7000-37FABE#reload force on rfs7000-37FABE
rfs7000-37FABE#
```

rename

Privileged Exec Mode Commands

Renames a file in the devices' file system

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
rename <OLD-FILE-NAME> <NEW-FILE-NAME>
```

Parameters

```
rename <OLD-FILE-NAME> <NEW-FILE-NAME>
```

<OLD-FILE-NAME>	Specify the file to rename.
<NEW-FILE-NAME>	Specify the new file name.

Example

```
rfs4000-229D58#dir
Directory of flash:/.

  drwx             Wed Jan 30 02:45:10 2013   log
  drwx             Sat Jan  1 00:00:09 2000   configs
  drwx             Sat Jan  1 00:00:08 2000   cache
  drwx             Wed Jan 16 22:26:53 2013   crashinfo
  drwx             Fri Feb 15 14:50:49 2013   testdir
  drwx             Wed Jan 16 22:57:14 2013   archived_logs
  drwx             Sat Jan  1 00:00:08 2000   upgrade
  drwx             Sat Jan  1 00:00:09 2000   hotspot
  drwx             Sat Jan  1 00:00:09 2000   floorplans
  drwx             Sat Jan  1 00:00:09 2000   startuplog
  -rw-   176128    Fri Feb 15 14:32:51 2013   out.tar

rfs4000-229D58#

rfs4000-229D58#rename flash:/testdir/ Final
rfs4000-229D58#

rfs4000-229D58#dir
Directory of flash:/.

  drwx             Wed Jan 30 02:45:10 2013   log
  drwx             Sat Jan  1 00:00:09 2000   configs
  drwx             Fri Feb 15 14:50:49 2013   Final
  drwx             Sat Jan  1 00:00:08 2000   cache
  drwx             Wed Jan 16 22:26:53 2013   crashinfo
  drwx             Wed Jan 16 22:57:14 2013   archived_logs
  drwx             Sat Jan  1 00:00:08 2000   upgrade
  drwx             Sat Jan  1 00:00:09 2000   hotspot
  drwx             Sat Jan  1 00:00:09 2000   floorplans
  drwx             Sat Jan  1 00:00:09 2000   startuplog
  -rw-   176128    Fri Feb 15 14:32:51 2013   out.tar

rfs4000-229D58#
```

rmdir

Privileged Exec Mode Commands

Deletes an existing directory from the file system (only empty directories can be removed)

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
rmdir <DIR>
```

Parameters

```
rmdir <DIR>
```

rmdir <DIR>	Specifies the directory name **NOTE:** The directory, specified by the <DIR> parameter, is removed from the file system.

Example

```
rfs4000-229D58#dir
Directory of flash:/.

  drwx             Wed Jan 30 02:45:10 2013   log
  drwx             Sat Jan  1 00:00:09 2000   configs
  drwx             Fri Feb 15 14:50:49 2013   Final
  drwx             Sat Jan  1 00:00:08 2000   cache
  drwx             Wed Jan 16 22:26:53 2013   crashinfo
  drwx             Wed Jan 16 22:57:14 2013   archived_logs
  drwx             Sat Jan  1 00:00:08 2000   upgrade
  drwx             Sat Jan  1 00:00:09 2000   hotspot
  drwx             Sat Jan  1 00:00:09 2000   floorplans
  drwx             Sat Jan  1 00:00:09 2000   startuplog
  -rw-   176128    Fri Feb 15 14:32:51 2013   out.tar

rfs4000-229D58#

rfs4000-229D58#rmdir Final
rfs4000-229D58#

rfs4000-229D58#dir
Directory of flash:/.

  drwx             Wed Jan 30 02:45:10 2013   log
  drwx             Sat Jan  1 00:00:09 2000   configs
  drwx             Sat Jan  1 00:00:08 2000   cache
  drwx             Wed Jan 16 22:26:53 2013   crashinfo
  drwx             Wed Jan 16 22:57:14 2013   archived_logs
  drwx             Sat Jan  1 00:00:08 2000   upgrade
  drwx             Sat Jan  1 00:00:09 2000   hotspot
  drwx             Sat Jan  1 00:00:09 2000   floorplans
```

```
  drwx             Sat Jan  1 00:00:09 2000   startuplog
  -rw-   176128    Fri Feb 15 14:32:51 2013   out.tar

rfs4000-229D58#
```

self

Privileged Exec Mode Commands

Enters the logged device's configuration context

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
self
```

Parameters

None

Example

```
rfs7000-37FABE#self
Enter configuration commands, one per line.  End with CNTL/Z.
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#
```

ssh

Privileged Exec Mode Commands

Opens a *Secure Shell* (SSH) connection between two network devices

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
ssh <IP/HOSTNAME> <USERNAME>
```

Parameters

```
ssh <IP/HOSTNAME> <USERNAME>
```

<IP/HOSTNAME>	Specify the remote systems's IP address or hostname.
<USERNAME>	Specify the name of the user requesting the SSH connection.

Usage Guidelines:

To exit the other device's context, use the command that is relevant to that device.

Example

```
rfs7000-37FABE#ssh 172.16.10.8 admin
admin@172.16.10.8's password:
rfs4000-229D58>
```

telnet

Privileged Exec Mode Commands

Opens a Telnet session between two network devices

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
telnet <IP/HOSTNAME> {<TCP-PORT>}
```

Parameters

```
telnet <IP/HOSTNAME> {<TCP-PORT>}
```

<IP/HOSTNAME>	Configures the remote system's IP address or hostname. The Telnet session will be established between the connecting system and the remote system. • <IP> – Specify the remote system's IP address or hostname.
<TCP-PORT>	Optional. Specify the *Transmission Control Protocol* (TCP) port.

Usage Guidelines:

To exit the other device's context, use the command relevant to that device.

Example

```
rfs4000-229D58#telnet 192.168.13.25

Entering character mode
Escape character is '^]'.


Brocade Mobility 71XX Access Point release 5.5.0.0-003D
br71xx-0F43D8 login: admin
Password:
br71xx-0F43D8>
```

terminal

Privileged Exec Mode Commands

Sets the number of characters per line, and the number of lines displayed within the terminal window

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
terminal [length|width] <0-512>
```

Parameters

```
terminal [length|width] <0-512>
```

length <0-512>	Sets the number of lines displayed on a terminal window • <0-512> – Specify a value from 0 - 512.
width <0-512>	Sets the width or number of characters displayed on the terminal window • <0-512> – Specify a value from 0 - 512.

Example

```
rfs7000-37FABE#terminal length 150
rfs7000-37FABE#

rfs7000-37FABE#terminal width 215
rfs7000-37FABE#
```

Related Commands:

no	Resets the width of the terminal window or the number of lines displayed on a terminal window

time-it

Privileged Exec Mode Commands

Verifies the time taken by a particular command between request and response

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
time-it <COMMAND>
```

Parameters

```
time-it <COMMAND>
```

time-it <COMMAND>	Verifies the time taken by a particular command to execute and provide a result • <COMMAND> – Specify the command name.

Example

```
rfs7000-37FABE#time-it config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
That took 0.00 seconds..
rfs7000-37FABE(config)#
```

traceroute

Privileged Exec Mode Commands

Traces the route to a defined destination

Use '--help' or '-h' to display a complete list of parameters for the traceroute command

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
traceroute <LINE>
```

Parameters

```
traceroute <LINE>
```

<LINE>	Traces the route to a destination IP address or hostname • <LINE> – Specify a traceroute argument. For example, "service traceroute-h".

Example

```
rfs7000-37FABE#traceroute 172.16.10.2
traceroute to 172.16.10.2 (172.16.10.2), 30 hops max, 38 byte packets
 1  172.16.10.1 (172.16.10.1)  3002.008 ms !H  3002.219 ms !H  3003.945 ms !H
rfs7000-37FABE#
```

upgrade

Privileged Exec Mode Commands

Upgrades a device's software image

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
upgrade [<FILE>|<URL>] {background|on <DEVICE-NAME>}
```

Parameters

```
upgrade [<FILE>|<URL>] {background|on <DEVICE-NAME>}
```

<FILE>	Specify the target firmware image location in the following format: cf:/path/file usb1:/path/file usb2:/path/file
<URL>	Specify the target firmware image location in the following format: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>:<passwd>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb<n>:/path/file
background	Optional. Performs upgrade in the background
on <DEVICE-NAME>	Optional. Upgrades the software image on a remote device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Example

```
rfs7000-37FABE#upgrade tftp://157.235.208.105:/img
var2 is 10 percent full
/tmp is 2 percent full
Free Memory 161896 kB
FWU invoked via Linux shell
Running from partition /dev/hda5, partition to

rfs7000-37FABE#upgrade tftp://157.125.208.235/img
Running from partition /dev/mtdblock7, partition to update is /dev/mtdblock6
```

Related Commands:

no	Removes a patch installed on a specified device

upgrade-abort

Privileged Exec Mode Commands

Aborts an ongoing software image upgrade

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
upgrade-abort {on <DEVICE-OR-DOMAIN-NAME>}
```

Parameters

```
upgrade-abort {on <DEVICE-OR-DOMAIN-NAME>}
```

upgrade-abort	Aborts an ongoing software image upgrade
on <DEVICE-OR-DOMAIN-NAME>	Optional. Aborts an ongoing software image upgrade on a specified device or domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

Example

```
rfs7000-37FABE#upgrade-abort on rfs7000-37FABE
Error: No upgrade in progress
rfs7000-37FABE#
```

watch

Privileged Exec Mode Commands

Repeats a specified CLI command at periodic intervals

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
watch <1-3600> <LINE>
```

Parameters

```
watch <1-3600> <LINE>
```

watch <1-3600>	Repeats a CLI command at a specified interval
<1-3600>	Select an interval from 1- 3600 seconds. Pressing CTRL-Z halts execution of the command
<LINE>	Specify the CLI command name.

Example

```
rfs7000-37FABE#watch 1 show clock
rfs7000-37FABE#
```

exit

Privileged Exec Mode Commands

Ends the current CLI session and closes the session window

For more information, see *exit*.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
exit
```

Parameters

None

Example

```
rfs7000-37FABE#exit
```

virtual-machine

Privileged Exec Mode Commands

Installs, configures, and monitors the status of third-party *virtual machines* (VMs)

In addition to the Brocade shipped VMs, Brocade Mobility RFS9510 series service platforms support the installation and administration of third-party VMs. However, the third-party VMs supported by these devices varies.

The third-party VMs supported on the Brocade Mobility RFS9510 are:

- ADSP
- TEAM-CMT

Use the virtual-machine command to install the third-party VMs, and configure parameters, such as install media type and location, number of *Virtual Central Processing Units* (VCPUS), VM memory, VM disk, number of *Virtual Network Interfaces* (VIFs), and *Virtual Networking Computing* (VNC) port.

Installing third-party VMs saves on hardware cost and provides a unified VM management interface.

This section is organized into the following sub-sections:

- Syntax *Brocade Mobility RFS9510*

Supported in the following platforms:

- Service Platforms — Brocade Mobility RFS9510

	`virtual-machine assign-usb-ports team-vowlan {on <DEVICE-NAME>}`
assign-usb-ports team-vowlan	Assigns USB ports to TEAM-VoWLAN on a specified device • on <DEVICE-NAME> – Optional. Specify the device name. Use the `no > virtual-machine > assign-usb-ports` to reassign the port to Mobility. TEAM-RLS VM cannot be installed when USB ports are assigned to TEAM-VoWLAN.

	`virtual-machine console [<VM-NAME>|team-urc|team-rls|team-vowlan]`
virtual-machine console	Connects to the VM's console, based on the parameters passed. Select one of the following console options: • <VM-NAME> – Connects to the console of the VM identified by the <VM-NAME> keyword. Specify the VM name. • team-urc – Connects to the VM TEAM-URC's (IP-PBX) console • team-rls – Connects to the VM TEAM *Radio Link Server's* (RLS) console • team-vowlan – Connects to the VM TEAM-VoWLAN's (Voice over WLAN) console

	`virtual-machine export <VM-NAME> [<FILE>|<URL>] {on <DEVICE-NAME>}`
virtual-machine export	Exports an existing VM image and settings. Use this command to export the VM to another device in the same domain. • <VM-NAME> – Specify the VM name. • <FILE> – Specify the location and name of the source file (VM image). The VM image is retrieved and exported from the specified location. • <URL> – Specify the destination location. This is the location to which the VM image is copied. Use one of the following formats to provide the destination path: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>:<passwd>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file • on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices • <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas. The VM should be in a stop state during the export process. If the destination is a device, the image is copied to a predefined location (VM archive)

	`virtual-machine install <VM-NAME> type [disk|iso disk-size <SIZE>|vm-archive] install-media [<FILE>|<URL>|<USB>] {autostart|memory|on|vcpus|vif-count|vnc}`
virtual-machine install	Installs the VM. The install command internally creates a VM template, consisting of the specified parameters, and starts the installation process. • <VM-NAME> – Specify the VM name. • type – Specify the install-media (image) type. The options are: • disk – Specifies the install media type as pre-installed OS disk image (located in the flash memory) • iso disk-size <SIZE> – Specifies the install media type as ISO file. This is a single file, which contains the OS bootable install media. • disk-size <SIZE> – If the install media type is ISO, specify the disk size in GB. • vm-archive – Specifies the install media type as VM archive. The VM archive file is a tar.gz file consisting of a pre-installed OS disk image and an associated configuration file. The configuration is a standard libvirt VM template consisting of VM specific information. After specifying the install media type, specify the location of the image. The image can be located in any of the following supported locations: FLASH, USB, or a remote location, such as http, ftp, sftp, tftp.
install-media [<FILE>|<URL>|<USB>]	Specifies the install media location • <FILE> – Specifies the install-media file is located on flash, for example flash:/cache • <URL> – Specifies the install-media file is located on a remote URL. Provide the URL using one of the following formats: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>:<passwd>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file • <USB> – Specifies the install-media file is located on a USB. Provide the USB path and file name using the following format: usb<n>:/path/file After specifying the image location, you may provide the following information: • autostart – Optional. Specifies whether to autostart the VM on system reboot • ignore – Enables autostart on each system boot/reboot • start – Disables autostart (default setting) • memory – Optional. Defines the VM memory size • <512-8192> – Specify the VM memory from 512 - 8192 MB. The default is 2048 MB. • on – Optional. Executes the command on a specified device • <DEVICE-NAME> – Specify the service platform name. • vcpus – Optional. Specifies the number of VCPUS for this VM • <1-4> – Specify the number of VCPUS from 1- 4. The default setting is 4. Contd...
	• vif-count – Optional. Configures or resets the VIF number for this VM • <0-2> – Specify the VIF number from 0 - 2. the default setting is 1. If assigning a virtual network interface for the VM, optionally specify the following parameters: • vif-mac – Sets the MAC index for the virtual interfaces 1 & 2. • vif-to-vmif – Maps the virtual interface (1 or 2) to the selected VMIF interface. Specify the VMIF interface index from 1 - 8. VMIFs are layer 2 interfaces on the Mobility bridge. Each custom VM can have up to a maximum of 2 virtual Ethernet interfaces. By default, these interfaces are internally connected to the Dataplane bridge through VMIF1, which is an untagged port with access VLAN 1. • vnc – Enables or disables VNC on the virtual interfaces 1 & 2 • vnc – Optional. Disables/enables VNC port. When enabled, provides remote access to VGA through the noVNC client. • disable – Disables VNC • enable – Enables VNC (default setting)

	`virtual-machine install [team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}`
virtual-machine install	Installs the VM. The install command internally creates a VM template, consisting of the specified parameters, and starts the installation process. Select one of the following options: • team-urc – Installs the VM TEAM-URC image • team-rls – Installs the VM TEAM-RLS image • team-vowlan – Installs the VM TEAM-VoWLAN image The following keywords are common to all of the above parameters: • on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices • <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas.

	`virtual-machine restart [<VM-NAME>|hard|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}`
virtual-machine restart	Restarts the VM • <VM-NAME> – Restarts the VM identified by the <VM-NAME> keyword • team-urc – Restarts the VM TEAM-URC • team-rls – Restarts the VM TEAM-RLS • team-vowlan – Restarts the VM TEAM-VoWLAN The following keywords are common to all of the above parameters: • on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices • <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas. The option '*hard*' forces the specified VM to restart.

```
virtual-machine set [autostart [ignore|start]|memory <512-8192>|vcpus <1-4>|
vif-count <0-2>|vif-mac <VIF-INDEX> <MAC-INDEX>|vif-to-vmif <VIF-INDEX>
<VMIF-INDEX>|
vnc [disable|enable]] [<VM-NAME>|team-urc|team-rls|team-vowlan] {on
<DEVICE-NAME>}
```

virtual-machine set	Configures the VM settings
	• autostart – Specifies whether to autostart the VM on system reboot
	  • ignore – Enables autostart on each system reboot
	  • start – Disables autostart
	• memory – Defines the VM memory size
	  • <512-8192> – Specify the VM memory from 512 - 8192 MB. The default is 1024 MB.
	• vcpus – Specifies the number of VCPUS for this VM
	  • <1-4> – Specify the number of VCPUS from 1- 4.
	• vif-count – Configures or resets the VM's VIFs
	  • <0-2> – Specify the VIF number from 0 - 2.
	• vif-mac – Configures the MAC address of the selected virtual network interface
	  • <1-2> – Select the VIF
	  • <1-8> – Specify the MAC index for the selected VIF
	  • <MAC> – Specify the customized MAC address for the selected VIF in the AA-BB-CC-DD-EE-FF format.
	Each VM has a maximum of two network interfaces (indexed 1 and 2, referred to as VIF). By default, each VIF is automatically assigned a MAC from the range allocated for that device. However, you can use the 'set' keyword to specify the MAC from within the allocated range. Each of these VIFs are mapped to a layer 2 port in the Dataplane (referred to as VMIF). These VMIFs are standard l2 ports on the DP bridge, supporting all VLAN and ACL commands. Mobility 5.5 supports up to a maximum of 8 VMIFs. By default, a VM's interface is always mapped to VMIF1. You can map a VIF to any of the 8 VMIFs. Use the vif-to-vmif command to map a VIF to a VMIF on the DP bridge.
	• vif-to-vmif – Maps the virtual interface (1 or 2) to the selected VMIF interface. Specify the VMIF interface index from 1 - 8.
	Mobility provides a dataplane bridge for external network connectivity for VMs. VM Interfaces define which IP address is associated with each VLAN ID the service platform is connected to and enables remote service platform administration. Each custom VM can have up to a maximum of two VM interfaces.
	By default, VM interfaces are internally connected to the dataplane bridge via VMIF1. VMIF1, by default, is an untagged port providing access to VLAN 1 to support the capability to connect the VM interfaces to any of the VMIF ports. This provides the flexibility to move a VM interface onto different VLANs as well as configure specific firewall and QOS rules.
	• vnc – Disables/enables VNC port option for an existing VM. When enabled, provides remote access to VGA through the noVNC client.
	  • disable – Disables VNC port
	  • enable – Enables VNC port
	Contd...

	After configuring the VM settings, identify the VM to apply the settings. • <VM-NAME> – Applies these settings to the VM identified by the <VM-NAME> keyword. Specify the VM name. • team-urc – Applies these settings to the VM TEAM-URC • team-rls – Applies these settings to the VM TEAM-RLS • team-vowlan – Applies these settings to the VM TEAM-VoWLAN

	`virtual-machine start [<VM-NAME>|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}`
virtual-machine start	Starts the VM, based on the parameters passed. Select one of the following options: • <VM-NAME> – Starts the VM identified by the <VM-NAME> keyword. Specify the VM name. • team-urc – Starts the VM TEAM-URC • team-rls – Starts the VM TEAM-RLS • team-vowlan – Starts the VM TEAM-VoWLAN The following keywords are common to all of the above parameters: • on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices • <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas.
	`virtual-machine stop [<VM-NAME>|hard|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}`
virtual-machine stop	Stops the VM, based on the parameters passed. Select one of the following options: • <VM-NAME> – Stops the VM identified by the <VM-NAME> keyword. Specify the VM name. • team-urc – Stops the VM TEAM-URC • team-rls – Stops the VM TEAM-RLS • team-vowlan – Stops the VM TEAM-VoWLAN The following keywords are common to all of the above parameters: • on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices • <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas. The option 'hard' forces the selected VM to shutdown
	`virtual-machine uninstall [<VM-NAME>|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}`
virtual-machine uninstall	Uninstalls the specified VM • <VM-NAME> – Uninstalls the VM identified by the <VM-NAME> keyword. Specify the VM name. • team-urc – Uninstalls the VM TEAM-URC • team-rls – Uninstalls the VM TEAM-RLS • team-vowlan – Uninstalls the VM TEAM-VoWLAN The following keywords are common to all of the above parameters: • on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices • <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas. This command releases the VM's resources, such as memory, VCPUS, VNC port, disk space, and removes the RF Domain reference from the system.

Syntax: Brocade Mobility RFS9510

```
virtual-machine
virtual-machine console [<VM-NAME>|adsp|team-cmt]
virtual-machine install [adsp|team-cmt] {on <DEVICE-NAME>}
virtual-machine restart [adsp|team-cmt] {on <DEVICE-NAME>}
virtual-machine set disk-size <100-500> adsp {on <DEVICE-NAME>}
virtual-machine set memory <512-8192> [adsp|team-cmt] {on <DEVICE-NAME>}
virtual-machine set Mobility-memory <12288-32739>
virtual-machine [start|stop] [adsp|team-cmt] {on <DEVICE-NAME>}
virtual-machine uninstall [adsp|team-cmt] {on <DEVICE-NAME>}
```

ParametersBrocade Mobility RFS9510

	`virtual-machine console [adsp|team-cmt]`
virtual-machine console	Connects to the ADSP or TEAM-CMT VM's console, based on the parameters passed. Select one of the following console options: • <VM-NAME> – Connects to the console of the VM identified by the <VM-NAME> keyword. Specify the VM name. • adsp – Connects to the *Air-Defense Services Platform* (ADSP) VM's management console • team-cmt – Connects to TEAM-CMT VM's management console When ADSP is running on the Brocade Mobility RFS9510 model service platforms, Mobility communicates with ADSP using a *single sign-on* (SSO) authentication mechanism. Once the user is logged in, Mobility gains access to ADSP without being prompted to login again at ADSP. However, the Mobility and ADSP databases are not synchronized. ADSP has its own user database, stored locally within its VM, which is accessed whenever a user logs directly into ADSP. Mobility and ADSP must be consistent in the manner events are reported up through a network hierarchy to ensure optimal interoperability and event reporting. To provide such consistency, Mobility has added support for an ADSP-like hierarchal tree. The tree resides within Mobility, and ADSP reads it from Mobility and displays the network hierarchy in its own ADSP interface. The hierarchal tree can also be used to launch ADSP modules (like Spectrum Analyzer) directly from Mobility. For more information on configuring Mobility tree-node structure, see *tree-node*.

	`virtual-machine install [adsp|team-cmt] {on <DEVICE-NAME>}`
virtual-machine install	Installs the ADSP or TEAM-CMT VM, based on the parameter passed • on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices • <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas. Before installing the ADSP VM, execute the upgrade command, giving the path and file name of the ADSP firmware image. This extracts the image on to the device (Brocade Mobility RFS9510) on which the command has been executed. On successful completion of this process, execute the reload command to reboot the device. Once the device has been successfully rebooted, execute the *virtual-machine > install > adsp* command. For example: `nx9500-6C874D#upgrade tftp://20.1.1.60/adsp-9.1.1Aug 20 15:12:41 2013: %DAEMON-6-INFO: lighttpd[2405]: 127.0.0.1 127.0.0.1:443 - "POST /mapi.fcgi HTTP/1.1" 200 192 "-" "-" -03-5.5.0.0-072B.img Aug 20 15:12:51 2013: nx9500-6C874D : %DIAG-6-NEW_LED_STATE: LED state message FIRMWARE_UPGRADE_STARTED from module led_msg Running from partition /dev/sda8 Validating image file header Extracting files (this may take some time).....Aug 20 15:12:53 2013: %DAEMON-6-INFO: lighttpd[2405]: 127.0.0.1 127.0.0.1:443 - "POST /mapi.fcgi HTTP/1.1" 200 923 "-" "-".....`

	`virtual-machine restart [adsp|team-cmt] {on <DEVICE-NAME>}`
virtual-machine restart	Restarts the ADSP or TEAM-CMT VM, based on the parameter passed • on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices • <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas.

	`virtual-machine set disk-size <100-500> adsp {on <DEVICE-NAME>}`
virtual-machine set disk-size	Sets the ADSP VM's disk size (in GB). Specify a value from 100 - 500 GB. • on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices • <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas. Stop the ADSP VM before executing this command.

	`virtual-machine set memory <512-8192> [adsp|team-cmt] {on <DEVICE-NAME>}`
virtual-machine set memory	Modifies the ADSP or TEAM-CMT VM's memory, in MB, based on the parameter passed. Specify a value from 512 - 8192 MB. • on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices • <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas.
	`virtual-machine set Mobility-memory <12288-32739>`
virtual-machine set Mobility-memory <12288-32739>	Specifies the Mobility memory size in MB. This command is applicable only to the Brocade Mobility RFS9510 service platforms. Use the *show > virtual-machine-configuration* command to view the configured memory allocation. Use the *show > virtual-machine-statistics* to view the current allocated memory allocation. • <12288-32739> – Specify a value from 12288 - 32739 MB. The default is 18432 MB. The new memory setting takes effect only after the next boot.
	`virtual-machine [start|stop] [adsp|team-cmt] {on <DEVICE-NAME>}`
virtual-machine [start|stop]	Starts/stops the ADSP or TEAM-CMT VM, based on the parameter passed • start – Starts the ADSP or TEAM-CMT VM. Use this command to boot a shut down VM (in a stop state). • stop – Stops a running ADSP or TEAM-CMT VM. Use this command to shut down a running VM. • on <DEVICE-NAME> – Optional. Executes the start/stop command on a specified device or devices • <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas.
	`virtual-machine uninstall [adsp|team-cmt] {on <DEVICE-NAME>}`
virtual-machine uninstall	Uninstalls the ADSP or TEAM-CMT VM based on the parameter passed • on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices • <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas.

Example

```
The following examples show the VM installation process:

Installation media: USB

<DEVICE>#virtual-machine install <VM-NAME> type iso disk-size 8 install-media
usb1://vms/win7.iso autostart start memory 512 vcpus 3 vif-count 2 vnc enable

Installation media: pre-installed disk image

<DEVICE>#virtual-machine install <VM-NAME> type disk install-media
flash:/vms/win7_disk.img autostart start memory 512 vcpus 3 vif-count 2
vnc-enable  on <DEVICE-NAME>

In the preceding example, the command is executed on the device identified by
the <DEVICE-NAME> keyword. In such a scenario, the disk-size is ignored if
specified. The VM has the install media as first boot device.

Installation media: VM archive

<DEVICE>#virtual-machine install type vm-archive install-media
flash:/vms/<VM-NAME> vcpus 3

In the preceding example, the default configuration attached with the VM
archive overrides any parameters specified.
```

```
Exporting an installed VM:

<DEVICE>#virtual-machine export <VM-NAME> <URL> on <DEVICE-NAME>

In the preceding example, the command copies the VM archive on to the URL (VM
should be in stop state).

nx4500-5CFA2B>virtual-machine install team-urc
Virtual Machine install team-urc command successfully sent.
nx4500-5CFA2B>
```

NOTE
Use the show > virtual-machine > [configuration|debugging|export|statistics] command to view installed VM details.

raid

Privileged Exec Mode Commands

Enables *Redundant Array of Independent Disks* (RAID) management

RAID is a group of one or more independent, physical drives, referred to as an array or drive group, These physically independent drives are linked together and appear as a single storage unit or multiple virtual drives. Replacing a single, large drive system with an array, improves performance (input and output processes are faster) and increases fault tolerance within the data storage system.

In an array, the drives can be organized in different ways, resulting in different RAID types. Each RAID type is identified by a number, which determines the RAID level. The common RAID levels are 0, 00, 1, 5, 6, 50 and 60. The Mobility MegaRAID implementation supports RAID-1, which provides data mirroring, but does not support data parity. RAID-1 consists of a two-drive array, where the data is simultaneously written on both drives, ensuring total data redundancy. In case of a drive failure the information on the other drive is used to rebuild the failed drive.

An array is said to be degraded when one of its drives has failed. A degraded array continues to function and can be rebooted using the one remaining functional drive. When a drive fails, the chassis sounds an alarm (if enabled), and the CLI prompt changes to “RAID degraded”. The failed drive is automatically replaced with a hot spare (provided a spare is installed). The spare is used to re-build the array.

Use this command to:

- Verify the current array status
- Start and monitor array consistency checks
- Retrieve date and time of the last consistency check
- Shut down drives before physically removing them
- Install new drives
- Assign drives as hot spares
- Identify a degraded drive
- Deactivate an alarm (triggered when a drive is removed from the array)

Syntax:

```
raid [check|install|locate|remove|silence|spare]

raid [check|silence]

raid [install|locate|remove|spare] drive <0-4>
```

Parameters

`raid [check|silence]`

check	Starts a consistency check on the RAID array. Use the *show > raid* command to view consistency check status. A consistency check verifies the data stored in the array. When regularly executed, it helps protect against data corruption, and ensures data redundancy. Consistency checks also warn of potential disk failures.
silence	Deactivates an alarm When enabled, an audible alarm is triggered when a drive in the array fails. The *silence* command deactivates the alarm (sound).

`raid [install|locate|remove|spare] drive <0-4>`

install <0-4>	Includes a new drive, inserted in one of the available slots, in the array. Specify the drive number. Drives 0 and 1 are the array drives. Drives 2, 3, and 4 are the hot spare drives. You can include the new drive in a degraded array, or enable it as a hot spare. If the array is in a degraded state, the re-build process is triggered and the new drive is used to repair the degraded array.
locate <0-4>	Enables LEDs to blink on a specified drive. Specify the drive number. Blinking LEDs enable you correctly locate a drive.
remove <0-4>	Removes (shuts downs) a disk from the array, before it is physically removed from its slot. Specify the drive number containing the disk. Use this command to also remove a hot spare.
spare <0-4>	Converts an unused drive into a hot spare. Specify the drive number.

Example

```
nx9500-6C874D#raid install drive 0
Error: Input Error: Drive 0 is already member of array, can't be added
nx9500-6C874D#
```

Chapter

GLOBAL CONFIGURATION COMMANDS

4

This chapter summarizes the global-configuration commands in the CLI command structure.

The term global indicates characteristics or features effecting the system as a whole. Use the Global Configuration Mode to configure the system globally, or enter specific configuration modes to configure specific elements (such as interfaces or protocols). Use the configure terminal command (under PRIV EXEC) to enter the global configuration mode.

The following example describes the process of entering the global configuration mode from the privileged EXEC mode:

```
<DEVICE># configure terminal
<DEVICE>(config)#
```

NOTE
The system prompt changes to indicate you are now in the global configuration mode. The prompt consists of the device host name followed by (config) and a pound sign (#).

Commands entered in the global configuration mode update the running configuration file as soon as they are entered. However, these changes are not saved in the startup configuration file until a *commit write memory* command is issued.

```
<DEVICE>(config)#?
Global configuration commands:
  aaa-policy                  Configure a
                              authentication/accounting/authorization policy
  aaa-tacacs-policy           Configure an
                              authentication/accounting/authorization TACACS
                              policy
  advanced-wips-policy        Configure a advanced-wips policy
  alias                       Alias
  br650                       Brocade Mobility 650 Access Point access point
  br6511                      Brocade Mobility 6511 Access Point access point
  br1220                      Brocade Mobility 1220 Access Point access point
  br71xx                      Brocade Mobility 71XX Access Point access point
  br81xx                      Brocade Mobility 1240 Access Point access point
  association-acl-policy      Configure an association acl policy
  auto-provisioning-policy    Configure an auto-provisioning policy
  captive-portal              Configure a captive portal
  clear                       Clear
  client-identity             Client identity (DHCP Device Fingerprinting)
  client-identity-group       Client identity group (DHCP Fingerprint
                              Database)
  clone                       Clone configuration object
  customize                   Customize the output of summary cli commands
  device                      Configuration on multiple devices
  device-categorization       Configure a device categorization object
  dhcp-server-policy          DHCP server policy
  dns-whitelist               Configure a whitelist
  event-system-policy         Configure a event system policy
  firewall-policy             Configure firewall policy
  global-association-list     Configure a global association list
```

```
  help                          Description of the interactive help system
  host                          Enter the configuration context of a device by
                                specifying its hostname
  igmp-snoop-policy             Create igmp snoop policy
  inline-password-encryption    Store encryption key in the startup
                                configuration file
  ip                            Internet Protocol (IP)
  l2tpv3                        L2tpv3 tunnel protocol
  mac                           MAC configuration
  management-policy             Configure a management policy
  meshpoint                     Create a new MESHPOINT or enter MESHPOINT
                                configuration context for one or more
  meshpoint-qos-policy          Configure a meshpoint quality-of-service policy
  mint-policy                   Configure the global mint policy
  nac-list                      Configure a network access control list
  no                            .
  nx45xx                        NX45XX integrated services platform
  nx65xx                        NX65XX integrated services platform
  nx9000                        NX9000 wireless controller
  passpoint-policy              Configure a passpoint policy
  password-encryption           Encrypt passwords in configuration
  profile                       Profile related commands - if no parameters are
                                given, all profiles are selected
  radio-qos-policy              Configure a radio quality-of-service policy
  radius-group                  Configure radius user group parameters
  radius-server-policy          Create device onboard radius policy
  radius-user-pool-policy       Configure Radius User Pool
  rename                        Clone configuration object
  rf-domain                     Create a RF Domain or enter rf-domain context
                                for one or more rf-domains
  rfs4000                       Brocade Mobility RFS4000 wireless controller
  rfs6000                       Brocade Mobility RFS6000 wireless controller
  rfs7000                       Brocade Mobility RFS7000 wireless controller
  role-policy                   Role based firewall policy
  routing-policy                Policy Based Routing Configuration
  self                          Config context of the device currently logged
                                into
  smart-cache-policy            Configure a content caching
  smart-rf-policy               Configure a Smart-RF policy
  url-list                      Configure a URL list
  wips-policy                   Configure a wips policy
  wlan                          Create a new WLAN or enter WLAN configuration
                                context for one or more WLANs
  wlan-qos-policy               Configure a wlan quality-of-service policy
  write                         Write running configuration to memory or
                                terminal


  clrscr                        Clears the display screen
  commit                        Commit all changes made in this session
  do                            Run commands from Exec mode
  end                           End current mode and change to EXEC mode
  exit                          End current mode and down to previous mode
  revert                        Revert changes
  service                       Service Commands
  show                          Show running system information

<DEVICE>(config)#
```

Global Configuration Commands

Table 2 summarizes the Global Configuration commands.

TABLE 2 Global Config Commands

Command	Description	Reference
aaa-policy	Configures a AAA policy	page 158
aaa-tacacs-policy	Configures AAA-TACACS policy	page 160
advanced-wips-policy	Configures an advanced WIPS policy	page 161
alias	Configures network, VLAN, and service aliases	page 162
br650	Adds an Brocade Mobility 650 Access Point to the network	page 169
br6511	Adds an Brocade Mobility 6511 Access Point to the network	page 169
br1220	Adds an Brocade Mobility 1220 Access Point to the network	page 170
br71xx	Adds an Brocade Mobility 71XX Access Point to the network	page 171
association-acl-policy	Configures an association ACL policy	page 174
auto-provisioning-policy	Configures an auto provisioning policy, which defines the process by which an access point discovers controllers and associates with it.	page 175
captive portal	Configures a captive portal	page 176
clear	Clears the event history	page 202
client-identity	Enables client identification through DHCP device fingerprinting	page 203
client-identity-group	Creates a new client identity group and enters its configuration mode	page 209
clone	Clones a specified configuration object	page 215
customize	Customizes the CLI command summary output	page 216
device	Specifies configuration on multiple devices	page 224
device-categorization	Configures a device categorization object	page 225
dhcp-server-policy	Configures a DHCP server policy	page 229
dns-whitelist	Configures a DNS whitelist	page 231
event-system-policy	Configures an event system policy	page 234
firewall-policy	Configures a firewall policy	page 246
global-association-list	Configures a global list of client MAC addresses	page 247
host	Sets the system's network name	page 249
inline-password-encryption	Stores the encryption key in the startup configuration file	page 250
ip	Configures *Internet Protocol* (IP) components	page 251
l2tpv3	Configures *Layer 2 Tunneling Protocol Version 3* (L2TPV3) tunnel policy	page 252
mac	Configures MAC access lists (goes to the MAC *Access Control List* (ACL) mode)	page 253
management-policy	Configures a management policy	page 254
meshpoint	Configures meshpoint related configuration commands	page 255
meshpoint-qos-policy	Configures a set of parameters that defines the *quality of service* (QoS)	page 257
mint-policy	Configures a MiNT security policy	page 258

TABLE 2 Global Config Commands

Command	Description	Reference
nac-list	Configures a network ACL	page 259
no	Negates a command or sets its default	page 263
passpoint-policy	Creates a new passpoint policy and enters its configuration mode	page 270
password-encryption	Enables password encryption	page 271
profile	Configures profile related commands	page 272
radio-qos-policy	Configures a radio qos policy	page 277
radius-group	Configures a RADIUS group	page 278
radius-server-policy	Configures a RADIUS server policy	page 279
radius-user-pool-policy	Configures a RADIUS user pool policy	page 280
rename	Renames and existing *top-level object* (TLO)	page 281
rf-domain	Creates an RF Domain	page 284
rfs4000	Adds an Brocade Mobility RFS4000 to the network	page 309
rfs6000	Adds an Brocade Mobility RFS6000 to the network	page 309
rfs7000	Adds an Brocade Mobility RFS7000 to the network	page 310
role-policy	Configures a role policy	page 310
routing-policy	Configures a routing policy	page 311
self	Displays a logged device's configuration context	page 312
smart-rf-policy	Configures a Smart RF policy	page 313
wips-policy	Configures a WIPS policy	page 314
wlan	Configures a wireless WLAN	page 315
wlan-qos-policy	Configures a WLAN QoS policy	page 369
smart-cache-policy	Enables content caching to allow temporary storing of frequently accessed content on an intermediate network device. This command is specific to the Brocade Mobility RFS9510 series service platforms.	page 371
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits current mode and moves to the PRIV EXEC mode	page 234
exit	Ends current mode and moves to the previous mode	page 387
help	Displays interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

aaa-policy

Global Configuration Commands

Configures an *Authentication, Accounting, and Authorization* (AAA) policy. This policy configures multiple servers for authentication and authorization. Up to six servers can be configured for providing AAA services.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
aaa-policy <AAA-POLICY-NAME>
```

Parameters

```
aaa-policy <AAA-POLICY-NAME>
```

<AAA-POLICY-NAME>	Specify the AAA policy name. If the policy does not exist, it is created.

Example

```
rfs7000-37FABE(config)#aaa-policy test
rfs7000-37FABE(config-aaa-policy-test)#?
AAA Policy Mode commands:
  accounting           Configure accounting parameters
  attribute            Configure RADIUS attributes in access and accounting
                       requests
  authentication       Configure authentication parameters
  health-check         Configure server health-check parameters
  mac-address-format   Configure the format in which the MAC address must be
                       filled in the Radius-Request frames
  no                   Negate a command or set its defaults
  proxy-attribute      Configure radius attribute behavior when proxying
                       through controller or rf-domain-manager
  server-pooling-mode  Configure the method of selecting a server from the
                       pool of configured AAA servers
  use                  Set setting to use

  clrscr               Clears the display screen
  commit               Commit all changes made in this session
  do                   Run commands from Exec mode
  end                  End current mode and change to EXEC mode
  exit                 End current mode and down to previous mode
  help                 Description of the interactive help system
  revert               Revert changes
  service              Service Commands
  show                 Show running system information
  write                Write running configuration to memory or terminal

rfs7000-37FABE(config-aaa-policy-test)#
```

Related Commands:

no	Removes an existing AAA policy

NOTE
For more information on the AAA policy commands, see *Chapter 8, AAA-POLICY*.

aaa-tacacs-policy

Global Configuration Commands

Configures AAA *Terminal Access Controller Access-Control System* (TACACS) policy. This policy configures multiple servers for authentication and authorization. A TACACS Authentication server should be configured when the server preference is authenticated server.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
aaa-tacacs-policy <AAA-TACACS-POLICY-NAME>
```

Parameters

```
aaa-tacacs-policy <AAA-TACACS-POLICY-NAME>
```

<AAA-TACACS-POLICY-NAME>	Specify the AAA-TACACS policy name. If the policy does not exist, it is created.

Example

```
rfs7000-37FABE(config)#aaa-tacacs-policy testpolicy
rfs7000-37FABE(config-aaa-tacacs-policy-testpolicy)#?
AAA TACACS Policy Mode commands:
  accounting      Configure accounting parameters
  authentication  Configure authentication parameters
  authorization   Configure authorization parameters
  no              Negate a command or set its defaults

  clrscr          Clears the display screen
  commit          Commit all changes made in this session
  do              Run commands from Exec mode
  end             End current mode and change to EXEC mode
  exit            End current mode and down to previous mode
  help            Description of the interactive help system
  revert          Revert changes
  service         Service Commands
  show            Show running system information
  write           Write running configuration to memory or terminal

rfs7000-37FABE(config-aaa-tacacs-policy-testpolicy)#
```

Related Commands:

no	Removes an existing AAA TACACS policy

NOTE
For more information on the AAA-TACACS policy commands, see *Chapter 26, AAA-TACACS-POLICY*.

advanced-wips-policy

Global Configuration Commands

Configures an advanced *Wireless Intrusion Prevention System* (WIPS) policy. WIPS prevents unauthorized access to a network.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
advanced-wips-policy <ADVANCED-WIPS-POLICY-NAME>
```

Parameters

```
advanced-wips-policy <ADVANCED-WIPS-POLICY-NAME>
```

<ADVANCED-WIPS-POLICY-NAME>	Specify the advanced WIPS policy name. If the policy does not exist, it is created.

Example

```
rfs7000-37FABE(config)#advanced-wips-policy test
rfs7000-37FABE(config-advanced-wips-policy-test)#?
Advanced WIPS policy Mode commands:
  event               Configure event detection
  no                  Negate a command or set its defaults
  server-listen-port  Configure local WIPS server listen port number
  terminate           Add a device to the list of devices to be terminated
  use                 Set setting to use

  clrscr              Clears the display screen
  commit              Commit all changes made in this session
  do                  Run commands from Exec mode
  end                 End current mode and change to EXEC mode
  exit                End current mode and down to previous mode
  help                Description of the interactive help system
  revert              Revert changes
  service             Service Commands
  show                Show running system information
  write               Write running configuration to memory or terminal

rfs7000-37FABE(config-advanced-wips-policy-test)#
```

Related Commands:

no	Removes an existing Advanced WIPS policy

NOTE
For more information on WIPS, see *Chapter 10, ADVANCED-WIPS-POLICY*.

alias

Global Configuration Commands

Configures network, VLAN, host, string, and network-service aliases

Aliases are objects having a unique name and content that is determined by the alias type (network, VLAN, and network-service).

A typical large enterprize network, consists of multiple sites (RF Domains) having similar configuration parameters with few elements that vary, such as networks or network ranges, hosts having different IP addresses, and VLAN IDs or URLs. These elements can be defined as aliases (object oriented wireless firewalls) and used across sites by applying overrides to the object definition. Using aliases results in a configuration that is easier to understand and maintain.

Multiple instances of an alias (same type and same name) can be defined at any of the following levels: global, RF Domain, profile, or device. An alias defined globally functions as a *top-level-object* (TLO). Global aliases are not mandatory, and can be defined at the domain-level, or profile, or device-level only. An alias defined on a device is applicable to that device only. An alias defined on a profile applies to every device using the profile. Similarly, aliases defined at the RF Domain level apply to all devices within that domain.

Aliases defined at any given level can be overridden at any of the next lower levels. For example, a global alias can be redefined on a selected set of RF Domains, profiles, or devices. Overrides applied at the device level take precedence.

Aliases can be classified as:

- address-range alias – Maps a name to a range of IP addresses. An address-range alias can be utilized at different deployments. For example, if an ACL defines a pool of network addresses as 192.168.10.10 through 192.168.10.100 for an entire network, and a remote location's network range is 172.16.13.20 through 172.16.13.110, the remote location's ACL can be overridden using an alias. At the remote location, the ACL works with the 172.16.13.20-110 address range. A new ACL need not be created specifically for the remote deployment location.
- host alias – Maps a name to a specific host (identified by its IP address. For example, 192.168.10.23). A host alias can be utilized at different deployments. For example, if a central network DNS server is set a static IP address, and a remote location's local DNS server is defined, this host can be overridden at the remote location. At the remote location, the network is functional with a local DNS server, but uses the name set at the central network. A new host need not be created at the remote location. This simplifies creating and managing hosts and allows an administrator to better manage specific local requirements.
- network alias – Maps a name to a network. A network alias can be utilized at different deployments. For example, if a central network ACL defines a network as 192.168.10.0/24, and a remote location's network range is 172.16.10.0/24, the ACL can be overridden at the remote location to suit their local (but remote) requirement. At the remote location, the ACL functions with the 172.16.10.0/24 network. A new ACL need not be created specifically for the remote deployment. This simplifies ACL definition and allows an administrator to better manage specific local requirements.

- network-group alias – Maps a name to a single or a range of addresses of devices, hosts, and network configurations. Network configurations are complete networks in the form 192.168.10.0/24 or IP address range in the form 192.168.10.10-192.168.10.20.

  A network-group alias can contain a maximum of eight (8) host entries, eight (8) network entries, and eight (8) IP address-range entries. A maximum of 32 network-group alias entries can be created.

  A network-group alias can be used in IP firewall rules to substitute hosts, subnets, and IP address ranges.

- network-service alias – Maps a name to service protocols and ports to match. Both source and destination ports are configurable. For each protocol, up to 2 source port ranges and up to 2 destination port ranges can be configured. A maximum of 4 protocol entries can be configured per network-service alias. When used with an ACL, the network-service alias defines the service-specific components of the ACL rule. Overrides can be applied to the service alias, at the device level, without modifying the ACL. Application of overrides to the service alias allows an ACL to be used across sites.

  Use a network-service alias to associate more than one IP address to a network interface, providing multiple connections to a network from a single IP node.

NOTE
When used with ACLs, network, network-group, and network-service aliases act as enhanced firewalls.

- vlan alias – maps a name to a VLAN ID. A VLAN alias can be used at different deployments. For example, if a named VLAN is defined as 10 for the central network, and the VLAN is set at 26 at a remote location, the VLAN can be overridden at the deployment location with an alias. At the remote deployment location, the network is functional with a VLAN ID of 26 but utilizes the name defined at the centrally managed network. A new VLAN need not be created specifically for the remote deployment.
- string alias – Maps a name to a specific string (for example, RF Domain name). A host alias can be utilized at different deployments. For example, if the main domain at a remote location is called *loc1.domain.com* and at another deployment location it is called *loc2.domain.com*, the alias can be overridden at the remote location to suit the local (but remote) requirement. At one remote location, the alias functions with the *loc1.domain.com* domain and at the other with the *loc2.domain.com* domain.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
alias [address-range|host|network|network-group|network-service|string|vlan]

alias address-range <ADDRESS-RANGE-ALIAS-NAME> <STARTING-IP> to <ENDING-IP>

alias host <HOST-ALIAS-NAME> <HOST-IP>
```

```
alias network <NETWORK-ALIAS-NAME> <NETWORK-ADDRESS/MASK>

alias network-group <NETWORK-GROUP-ALIAS-NAME> [address-range|host|network]
alias network-group <NETWORK-GROUP-ALIAS-NAME> [address-range <STARTING-IP> to
          <ENDING-IP> {<STARTING-IP> to <ENDING-IP>}|host <HOST-IP>
{<HOST-IP>}|
          network <NETWORK-ADDRESS/MASK> {<NETWORK-ADDRESS/MASK>}]

alias network-service <NETWORK-SERVICE-ALIAS-NAME> proto
[<0-254>|<WORD>|eigrp|gre|
          igmp|igp|ospf|vrrp]
{(<1-65535>|<WORD>|bgp|dns|ftp|ftp-data|gopher|https|ldap|nntp|
          ntp|pop3|proto|sip|smtp|sourceport|ssh|telnet|tftp|www)}

alias network-service <NETWORK-SERVICE-ALIAS-NAME> proto
[<0-254>|<WORD>|eigrp|gre|
          igmp|igp|ospf|vrrp]
{(<1-65535>|<WORD>|bgp|dns|ftp|ftp-data|gopher|https|ldap|nntp|
          ntp|pop3|proto|sip|smtp|sourceport
[<1-65535>|<WORD>]|ssh|telnet|tftp|www)}

alias string <STRING-ALIAS-NAME> <LINE>

alias vlan <VLAN-ALIAS-NAME> <1-4094>
```

Parameters

`alias address-range <ADDRESS-RANGE-ALIAS-NAME> <STARTING-IP> to <ENDING-IP>`

address-range <ADRESS-RANGE-ALIAS-NAME>	Creates a address range alias, defining a range of IP addresses • <ADRESS-RANGE-ALIAS-NAME> – Specify the address range alias name. Alias name should begin with '$'.
<STARTING-IP> to <ENDING-IP>	Associates a range of IP addresses with this address range alias • <STARTING-IP> – Specify the first IP address in the range. • to <ENDING-IP> – Specify the last IP address in the range.

`alias host <HOST-ALIAS-NAME> <HOST-IP>`

host <HOST-ALIAS-NAME>	Creates a host alias, defining a single network host • <HOST-ALIAS-NAME> – Specify the host alias name. Alias name should begin with '$'.
<HOST-IP>	Associates the network host's IP address with this host alias. For example, 'alias host $HOST 1.1.1.100'. In this example, the host alias name is: *$HOST* **and** the host IP address it is mapped to is: *1.1.1.100*. • <HOST-IP> – Specify the network host's IP address.

`alias network <NETWORK-ALIAS-NAME> <NETWORK-ADDRESS/MASK>`

network <NETWORK-ALIAS-NAME>	Creates a network alias, defining a single network address • <NETWORK-ALIAS-NAME> – Specify the network alias name. Alias name should begin with '$'.
<NETWORK-ADDRESS/MASK>	Associates a single network with this network alias. For example, 'alias network $NET 1.1.1.0/24'. In this example, the network alias name is: *$NET* **and** the network it is mapped to is: *1.1.1.0/24*. • <NETWORK-ADDRESS/MASK> – Specify the network's address and mask.

	`alias network-group <NETWORK-GROUP-ALIAS-NAME> [address-range <STARTING-IP> to <ENDING-IP> {<STARTING-IP> to <ENDING-IP>}|host <HOST-IP> {<HOST-IP>}| network <NETWORK-ADDRESS/MASK> {<NETWORK-ADDRESS/MASK>}]`
network <NETWORK-GROUP-ALIAS-NAME>	Creates a network-group alias • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name. Alias name should begin with '$'. The network-group aliases are used in ACLs, to define the network-specific components. ACLs using aliases can be used across sites by re-defining the network-group alias elements at the device or profile level. After specifying the name, specify the following: a range of IP addresses, host addresses, or a range of network addresses.
address-range <STARTING-IP> to <ENDING-IP> {<STARTING-IP> to <ENDING-IP>}	Associates a range of IP addresses with this network-group alias • <STARTING-IP> – Specify the first IP address in the range. • to <ENDING-IP> – Specify the last IP address in the range. • <STARTING-IP> to <ENDING-IP> – Optional. Specifies more than one range of IP addresses. A maximum of eight (8) IP address ranges can be configured.
host <HOST-IP> {<HOST-IP>}	Associates a single or multiple hosts with this network-group alias • <HOST-IP> – Specify the hosts' IP address. • <HOST-IP> – Optional. Specifies more than one host. A maximum of eight (8) hosts can be configured.
network <NETWORK-ADDRESS/MASK> {<NETWORK-ADDRESS/MASK>}	Associates a single or multiple networks with this network-group alias • <NETWORK-ADDRESS/MASK> – Specify the network's address and mask. • <NETWORK-ADDRESS/MASK> – Optional. Specifies more than one network. A maximum of eight (8) networks can be configured.
	`alias network-service <NETWORK-SERVICE-ALIAS-NAME> proto [<0-254>|<WORD>|eigrp|gre| igmp|igp|ospf|vrrp] {(<1-65535>|<WORD>|bgp|dns|ftp|ftp-data|gopher|https|ldap|nntp| ntp|pop3|proto|sip|smtp|sourceport [<1-65535>|<WORD>]|ssh|telnet|tftp|www)}`
alias network-service <NETWORK-SERVICE-ALIAS-NAME>	Configures an alias that specifies available network services and the corresponding source and destination software ports • <NETWORK-SERVICE-ALIAS-NAME> – Specify a network-service alias name. Alias name should begin with '$'. Network-service aliases are used in ACLs, to define the service-specific components. ACLs using aliases can be used across sites by re-defining the network-service alias elements at the device or profile level.

proto [<0-254>|<WORD>|eigrp|gre|igmp|igp|ospf|vrrp]	Use one of the following options to associate an Internet protocol with this network-service alias: • <0-254> – Identifies the protocol by its number. Specify the protocol number from 0 - 254. This is the number by which the protocol is identified in the *Protocol* field of the IPv4 header and the *Next Header* field of IPv6 header. For example, the *User Datagram Protocol's* (UDP) designated number is 17. • <WORD> – Identifies the protocol by its name. Specify the protocol name. • eigrp – Selects *Enhanced Interior Gateway Routing Protocol* (EIGRP). The protocol number 88. • gre – Selects *Generic Routing Encapsulation* (GRE). The protocol number is 47. • igmp – Selects *Internet Group Management Protocol* (IGMP). The protocol number is 2. • igp – Selects *Interior Gateway Protocol* (IGP). The protocol number is 9. • ospf – Selects *Open Shortest Path First* (OSPF). The protocol number is 89. • vrrp – Selects *Virtual Router Redundancy Protocol* (VRRP). The protocol number is 112.

{(<1-65535>|<WORD>|bgp|dns|ftp|ftp-data|gopher|https|ldap|nntp|ntp|pop3|proto|sip|smtp|sourceport [<1-65535>|<WORD>]|ssh|telnet|tftp|www)}	After specifying the protocol, you may configure a destination port for this service. These keywords are recursive and you can configure multiple protocols and associate multiple destination and source ports.
	• <1-65535> – Optional. Configures a destination port number from 1 - 65535
	• <WORD> – Optional. Identifies the destination port by the service name provided. For example, the *secure shell* (SSH) service uses TCP port 22.
	• bgp – Optional. Configures the default *Border Gateway Protocol* (BGP) services port (179)
	• dns – Optional. Configures the default *Domain Name System* (DNS) services port (53)
	• ftp – Optional. Configures the default *File Transfer Protocol* (FTP) control services port (21)
	• ftp-data – Optional. Configures the default FTP data services port (20)
	• gopher – Optional. Configures the default gopher services port (70)
	• https – Optional. Configures the default HTTPS services port (443)
	• ldap – Optional. Configures the default *Lightweight Directory Access Protocol* (LDAP) services port (389)
	• nntp – Optional. Configures the default Newsgroup (NNTP) services port (119)
	• ntp – Optional. Configures the default *Network Time Protocol* (NTP) services port (123)
	• POP3 – Optional. Configures the default *Post Office Protocol* (POP3) services port (110)
	• proto – Optional. Use this option to select another Internet protocol in addition to the one selected in the previous step.
	• sip – Optional. Configures the default *Session Initiation Protocol* (SIP) services port (5060)
	• smtp – Optional. Configures the default *Simple Mail Transfer Protocol* (SMTP) services port (25)
	• sourceport [<1-65535>|<WORD>] – Optional. After specifying the destination port, you may specify a single or range of source ports.
	  • <1-65535> – Specify the source port from 1 - 65535.
	  • <WORD> – Specify the source port range, for example 1-10.
	• ssh – Optional. Configures the default SSH services port (22)
	• telnet – Optional. Configures the default Telnet services port (23)
	• tftp – Optional. Configures the default *Trivial File Transfer Protocol* (TFTP) services port (69)
	• www – Optional. Configures the default HTTP services port (80)

```
alias string <STRING-ALIAS-NAME> <LINE>
```

alias string <STRING-ALIAS-NAME>	Creates a string alias identified by the <STRING-ALIAS-NAME> keyword • <STRING-ALIAS-NAME> – Specify the string alias name. • <LINE> – Specify the string value. String aliases map a name to an arbitrary string value. For example, 'alias string $DOMAIN test.brocade.com'. In this example, the string alias name is: *$DOMAIN* and the string value it is mapped to is: *test.brocade.com*. In this example, the string alias refers to a domain name. Alias name should begin with '$'.

```
alias vlan <VLAN-ALIAS-NAME> <1-4094>
```

alias vlan <VLAN-ALIAS-NAME>	Creates a VLAN alias identified by the <VLAN-ALIAS-NAME> keyword • <VLAN-ALIAS-NAME> – Specify the VLAN alias name. Alias name should begin with '$'.
<1-4094>	Maps the VLAN alias to a VLAN ID • <1-4094> – Specify the VLAN ID from 1 - 4094.

Example

```
rfs4000-229D58(config)#alias address-range $TestAddRanAlias 192.168.13.10 to
192.168.13.13
rfs4000-229D58(config)#

rfs4000-229D58(config)#alias network $TestNetworkAlias 192.168.13.0/24
rfs4000-229D58(config)#

rfs4000-229D58(config)#alias host $TestHostAlias 192.168.13.10
rfs4000-229D58(config)#

rfs4000-229D58(config)#alias vlan $TestVLANAlias 1
rfs4000-229D58(config)#

rfs4000-229D58(config)#alias network-group $TestNetGrpAlias address-range
192.168.13.7 to 192.168.13.16 192.168.13.20 to 192.168.13.25
rfs4000-229D58(config)#commit

rfs4000-229D58(config)#alias network-group $TestNetGrpAlias network
192.168.13.0/24 192.168.16.0/24
rfs4000-229D58(config)#commit

rfs4000-229D58(config)#alias network-service $NetworkServAlias proto 17
rfs4000-229D58(config)#commit

rfs4000-229D58(config)#show context
!
! Configuration of Brocade Mobility RFS4000 version 5.5.0.0-053B
!
!
version 2.3
!
!
alias network-group $TestNetGrpAlias network 192.168.13.0/24 192.168.16.0/24
alias network-group $TestNetGrpAlias address-range 192.168.13.7 to
192.168.13.16 192.168.13.20 to 192.168.13.25
!
alias network $TestNetworkAlias 192.168.13.0/24
!
alias host $TestHostAlias 192.168.13.10
!
alias address-range $TestAddRanAlias 192.168.13.10 to 192.168.13.13
!
alias network-service $NetworkServAlias proto udp
!
alias vlan $TestVLANAlias 1
!
ip access-list BROADCAST-MULTICAST-CONTROL
 permit tcp any any rule-precedence 10 rule-description "permit all TCP
traffic"
--More--
```

```
rfs4000-229D58(config)#

Example 1:
rfs4000-229D58(config)# alias network-group $test host 192.168.1.10
192.168.1.11
rfs4000-229D58(config)# alias network-group $test network 192.168.2.0/24
192.168.3.0/24
rfs4000-229D58(config)# alias network-group $test address-range 192.168.4.10
to 192.168.4.20
```

In the preceding example, the network-group alias ‘$test’ includes hosts 192.168.1.10 and 192.168.1.11, networks 192.168.2.0/24 and 192.168.3.0/24 and address-range 192.168.4.10 to 192.168.4.20.

```
Example 2:
rfs4000-229D58(config)#alias network-service $kerberos proto tcp 749 750 80
proto tcp sourceport 20 proto udp 68 sourceport 67
rfs4000-229D58(config)#commit
```

In the preceding example, the network-service alias ‘$kerberos’ is configured to allow following traffic:

- TCP traffic to destination ports 749, 750, and 80
- TCP traffic from source port 20
- UDP traffic to destination port 68 and from source port 67

```
rfs4000-229D58(config)#alias string $DOMAIN test.brocade.com

rfs4000-229D58(config)#show context
!
! Configuration of Brocade Mobility RFS4000 version 5.5.0.0-071B
!
!
version 2.3
!
!
.....................................................................
!
 client-identity Android-4-1-X precedence 1700
 client-identity Android-4-2-X precedence 1800
!
alias string $DOMAIN test.brocade.com'
!
ip access-list BROADCAST-MULTICAST-CONTROL
 permit tcp any any rule-precedence 10 rule-description "permit all TCP
traffic"
 permit udp any eq 67 any eq dhcpc rule-precedence 11 rule-description "permit
DHCP replies"
 deny udp any range 137 138 any range 137 138 rule-precedence 20
rule-description "deny windows netbios"
 deny ip any 224.0.0.0/4 rule-precedence 21 rule-description "deny IP
multicast"
 deny ip any host 255.255.255.255 rule-precedence 22 rule-description "deny IP
l
  --More--
```

Related Commands:

no	Removes an existing network, VLAN, service, or string alias

br650

Global Configuration Commands

Adds an Brocade Mobility 650 Access Point to the network. If a profile for the AP is not available, a new profile is created.

Supported in the following platforms:

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
br650 <MAC>
```

Parameters

```
br650 <MAC>
```

<MAC>	Specify the Brocade Mobility 650 Access Point's MAC address.

Example

```
rfs7000-37FABE(config)#br650 5C-0E-8B-34-81-BC
rfs7000-37FABE(config-device-5C-0E-8B-34-81-BC)#

rfs7000-37FABE(config)#show wireless br configured
------------------------------------------------------------------------------
----------
IDX         NAME                MAC               PROFILE       RF-DOMAIN
ADOPTED-BY
------------------------------------------------------------------------------
----------
  1    br7131-889EC4      00-15-70-88-9E-C4   default-br7131    default
un-adopted
5    br650-3481BC       5C-0E-8B-34-81-BC   default-br650     default
un-adopted
------------------------------------------------------------------------------
----------
rfs7000-37FABE(config)#
```

Related Commands:

no	Removes an Brocade Mobility 650 Access Point from the network

br6511

Global Configuration Commands

Adds an Brocade Mobility 6511 Access Point to the network. If a profile for the AP is not available, a new profile is created.

Supported in the following platforms:

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
br6511 <MAC>
```

Parameters

```
br6511 <MAC>
```

<MAC>	Specify the Brocade Mobility 6511 Access Point's MAC address.

Example

```
rfs7000-37FABE(config)#br6511 5C-0E-8B-08-45-6A
rfs7000-37FABE(config-device-5C-0E-8B-08-45-6A)#

rfs7000-37FABE(config)#show wireless br configured
------------------------------------------------------------------------------
----------
IDX         NAME                MAC              PROFILE       RF-DOMAIN
ADOPTED-BY
------------------------------------------------------------------------------
----------
  1    br7131-889EC4      00-15-70-88-9E-C4   default-br7131    default
un-adopted
5    br650-3481BC       5C-0E-8B-34-81-BC   default-br650     default
un-adopted
  6    br6511-08456A      5C-0E-8B-08-45-6A   default-br6511    default
un-adopted
------------------------------------------------------------------------------
----------
rfs7000-37FABE(config)#
```

Related Commands:

no	Removes an Brocade Mobility 6511 Access Point from the network

br1220

Global Configuration Commands

Adds an Brocade Mobility 1220 Access Point to the network. If a profile for the AP is not available, a new profile is created.

Supported in the following platforms:

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
br1220 <MAC>
```

Parameters

```
br1220 <MAC>
```

<MAC>	Specify the Brocade Mobility 1220 Access Point's MAC address.

Example

```
rfs7000-37FABE(config)#br1220 5C-0E-8B-7B-F2-24
rfs7000-37FABE(config-device-5C-0E-8B-7B-F2-24)#

rfs7000-37FABE(config)#show wireless br configured
------------------------------------------------------------------------------
----------
IDX         NAME                MAC              PROFILE       RF-DOMAIN
ADOPTED-BY
------------------------------------------------------------------------------
----------
  1    br7131-889EC4      00-15-70-88-9E-C4   default-br7131    default
un-adopted
5    br650-3481BC       5C-0E-8B-34-81-BC   default-br650     default
un-adopted
  6    br6511-08456A      5C-0E-8B-08-45-6A   default-br6511    default
un-adopted
8    br1220-7BF224      5C-0E-8B-7B-F2-24   default-br1220    default
un-adopted
------------------------------------------------------------------------------
----------
rfs7000-37FABE(config)#
```

Related Commands:

no	Removes an Brocade Mobility 1220 Access Point from the network

br71xx

Global Configuration Commands

Adds an Brocade Mobility 71XX Access Point series to the network. If a profile for the AP is not available, a new profile is created.

Supported in the following platforms:

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
br71xx <MAC>
```

Parameters

```
br71xx <MAC>
```

<MAC>	Specify the Brocade Mobility 71XX Access Point's MAC address.

Example

```
rfs7000-37FABE(config)#br71xx 00-23-68-99-BF-A8
```

```
rfs7000-37FABE(config-device-00-23-68-99-BF-A8)#

rfs7000-37FABE(config)#show wireless br configured
------------------------------------------------------------------------------
----------
IDX         NAME                MAC              PROFILE       RF-DOMAIN
ADOPTED-BY
------------------------------------------------------------------------------
----------
  1    br7131-889EC4      00-15-70-88-9E-C4   default-br7131    default
un-adopted
5    br650-3481BC       5C-0E-8B-34-81-BC   default-br650     default
un-adopted
  6    br6511-08456A      5C-0E-8B-08-45-6A   default-br6511    default
un-adopted
8    br1220-7BF224      5C-0E-8B-7B-F2-24   default-br1220    default
un-adopted
11   br7131-99BFA8      00-23-68-99-BF-A8   default-br71xx    default
un-adopted
------------------------------------------------------------------------------
----------
rfs7000-37FABE(config)#
```

Related Commands:

no	Removes an Brocade Mobility 71XX Access Point from the network

br81xx

Global Configuration Commands

Adds an Brocade Mobility 1240 Access Point series to the network. If a profile for the AP is not available, a new profile is created.

Supported in the following platforms:

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
br81xx <MAC>
```

Parameters

```
br81xx <MAC>
```

<MAC>	Specify the Brocade Mobility 1240 Access Point's MAC address.

Example

```
rfs7000-37FABE(config)#br81xx C4-01-FA-BE-F1-16
rfs7000-37FABE(config-device-C4-01-FA-BE-F1-16)#

rfs7000-37FABE(config)#show wireless br configured
------------------------------------------------------------------------------
-------------
```

```
IDX         NAME                MAC               PROFILE       RF-DOMAIN
ADOPTED-BY
-------------------------------------------------------------------------------
-------------
  1    br7131-889EC4      00-15-70-88-9E-C4   default-br7131    default
un-adopted
5    br650-3481BC       5C-0E-8B-34-81-BC   default-br650     default
un-adopted
  6    br6511-08456A      5C-0E-8B-08-45-6A   default-br6511    default
un-adopted
8    br1220-7BF224      5C-0E-8B-7B-F2-24   default-br1220    default
un-adopted
11   br7131-99BFA8      00-23-68-99-BF-A8   default-br71xx    default
un-adopted
  12   br8132-BEF116      C4-01-FA-BE-F1-16   default-br81xx    default
un-adopted
-------------------------------------------------------------------------------
-------------
rfs7000-37FABE(config)#
```

Related Commands:

no	Removes an Brocade Mobility 1240 Access Point from the network

ap82xx

Global Configuration Commands

Adds an AP82XX series to the network. If a profile for the AP is not available, a new profile is created.

Supported in the following platforms:

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
ap82xx <MAC>
```

Parameters

```
ap82xx <MAC>
```

<MAC>	Specify the AP82XX's MAC address.

Example

```
rfs7000-37FABE(config)#ap82xx 6C-90-CD-02-54-21
rfs7000-37FABE(config-device-6C-90-CD-02-54-21)#

rfs7000-37FABE(config)#show wireless br configured
-------------------------------------------------------------------------------
----------
IDX         NAME                MAC               PROFILE       RF-DOMAIN
ADOPTED-BY
-------------------------------------------------------------------------------
----------
```

```
  1    br7131-889EC4      00-15-70-88-9E-C4   default-br7131    default
un-adopted
5    br650-3481BC       5C-0E-8B-34-81-BC   default-br650     default
un-adopted
  6    br6511-08456A      5C-0E-8B-08-45-6A   default-br6511    default
un-adopted
8    br1220-7BF224      5C-0E-8B-7B-F2-24   default-br1220    default
un-adopted
11   br7131-99BFA8      00-23-68-99-BF-A8   default-br71xx    default
un-adopted
  12   br8132-BEF116      C4-01-FA-BE-F1-16   default-br81xx    default
un-adopted
-------------------------------------------------------------------------------
----------
rfs7000-37FABE(config)#
```

Related Commands:

no	Removes an AP82XX from the network

association-acl-policy

Global Configuration Commands

Configures an association ACL policy. This policy defines a list of devices allowed or denied access to the network.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
association-acl-policy <ASSOCIATION-ACL-POLICY-NAME>
```

Parameters

```
association-acl-policy <ASSOCIATION-ACL-POLICY-NAME>
```

<ASSOCIATION-ACL-POLICY-NAME>	Specify the association ACL policy name. If the policy does not exist, it is created.

Example

```
rfs7000-37FABE(config)#association-acl-policy test
rfs7000-37FABE(config-assoc-acl-test)#?
Association ACL Mode commands:
  deny     Specify MAC addresses to be denied
  no       Negate a command or set its defaults
  permit   Specify MAC addresses to be permitted

  clrscr   Clears the display screen
  commit   Commit all changes made in this session
```

```
  do       Run commands from Exec mode
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  revert   Revert changes
  service  Service Commands
  show     Show running system information
  write    Write running configuration to memory or terminal

rfs7000-37FABE(config-assoc-acl-test)#
```

Related Commands:

no	Resets values or disables commands

NOTE
For more information on the association-acl-policy, see *Chapter 11, ASSOCIATION-ACL-POLICY*.

auto-provisioning-policy

Global Configuration Commands

Configures an auto provisioning policy. This policy configures the automatic provisioning of device adoption. The policy configures how an AP is adopted based on its type.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
auto-provisioning-policy <AUTO-PROVISIONING-POLICY-NAME>
```

Parameters

```
auto-provisioning-policy <AUTO-PROVISIONING-POLICY-NAME>
```

<AUTO-PROVISIONING-POLICY-NAME>	Specify the auto provisioning policy name. If the policy does not exist, it is created.

Example

```
rfs7000-37FABE(config)#auto-provisioning-policy test
rfs7000-37FABE(config-auto-provisioning-policy-test)#?
Auto-Provisioning Policy Mode commands:
  adopt             Add rule for device adoption
  default-adoption  Adopt devices even when no matching rules are found.
                    Assign default profile and default rf-domain
  deny              Add rule to deny device adoption
  no                Negate a command or set its defaults
  redirect          Add rule to redirect device adoption
  upgrade           Add rule for device upgrade
```

```
  clrscr            Clears the display screen
  commit            Commit all changes made in this session
  do                Run commands from Exec mode
  end               End current mode and change to EXEC mode
  exit              End current mode and down to previous mode
  help              Description of the interactive help system
  revert            Revert changes
  service           Service Commands
  show              Show running system information
  write             Write running configuration to memory or terminal

rfs7000-37FABE(config-auto-provisioning-policy-test)#
```

Related Commands:

no	Removes an existing Auto Provisioning policy

NOTE
For more information on the association-acl-policy, see *Chapter 9, AUTO-PROVISIONING-POLICY*.

captive portal

Global Configuration Commands

A captive portal provides secure guest access and authentication services within the network. The following table lists the command to enter the captive portal configuration mode.

Command	Description	Reference
captive-portal	Creates a new captive portal and enters its configuration mode	page 176
captive-portal-mode commands	Summarizes captive portal configuration commands	page 178

captive-portal

captive portal

Configures a captive portal

A captive portal provides secure access using a standard Web browser. Captive portals provide authenticated access by capturing and re-directing a wireless user's Web browser session to a captive portal login page where the user must enter valid credentials to access to the wireless network. Once logged into the captive portal, additional Acknowledgment, Agreement, Welcome, No Service, and Fail pages provide the administrator options to customize the screen flow and user appearance.

Captive portals are recommended for providing guests or visitors authenticated access to network resources when 802.1X EAP is not a viable option. Captive portal authentication does not provide end-user data encryption, but it can be used with static WEP, WPA-PSK or WPA2-PSK encryption.

Authentication for captive portal access requests is performed using a username and password pair, authenticated by an integrated RADIUS server. Authentication for private network access is conducted either locally on the requesting wireless client, or centrally at a datacenter.

Captive portals use a Web provisioning tool to create guest user accounts directly on the controller, service platform, or access point. The connection medium defined for the Web connection is either HTTP or HTTPS. Both HTTP and HTTPS use a request and response procedure to disseminate information to and from requesting wireless clients.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
captive-portal <CAPTIVE-PORTAL-NAME>
```

Parameters

```
captive-portal <CAPTIVE-PORTAL-NAME>
```

<CAPTIVE-PORTAL-NAME>	Specify the captive portal name. If the captive portal does not exist, it is created.

Example

```
rfs7000-37FABE(config)#captive-portal test
rfs7000-37FABE(config-captive-portal-test)#?
Captive Portal Mode commands:
  access-time               Allowed access time for the client. Used when
                            there is no session time in radius response
  access-type               Access type of this captive portal
  accounting                Configure how accounting records are created for
                            this captive portal policy
  bypass                    Bypass captive portal
  connection-mode           Connection mode for this captive portal
  custom-auth               Custom user information
  data-limit                Enforce data limit for clients
  inactivity-timeout        Inactivity timeout in seconds. If a frame is not
                           received from client for this amount of time, then
                            current session will be removed
  logout-fqdn               Configure the FQDN address to logout the session
                            from client
  no                        Negate a command or set its defaults
  post-authentication-vlan  Configure post authentication vlan for captive
                            portal users
  radius-vlan-assignment    Enable radius vlan assignment for captive portal
                            users
  redirection               Configure connection redirection parameters
  server                    Configure captive portal server parameters
  simultaneous-users        Particular username can only be used by a certain
                            number of MAC addresses at a time
  terms-agreement           User needs to agree for terms and conditions
  use                       Set setting to use
  webpage                   Configure captive portal webpage parameters
  webpage-auto-upload       Enable automatic upload of advanced webpages
  webpage-location          The location of the webpages to be used for
                            authentication. These pages can either be hosted
                            on the system or on an external web server.
```

```
clrscr                  Clears the display screen
commit                  Commit all changes made in this session
do                      Run commands from Exec mode
end                     End current mode and change to EXEC mode
exit                    End current mode and down to previous mode
help                    Description of the interactive help system
revert                  Revert changes
service                 Service Commands
show                    Show running system information
write                   Write running configuration to memory or terminal

rfs7000-37FABE(config-captive-portal-test)#
```

Related Commands:

no	Removes an existing captive portal

captive-portal-mode commands

captive portal

The following table summarizes captive portal configuration mode commands.

Command	Description	Reference
access-time	Defines a client's access time. It is used when no session time is defined in the RADIUS response.	page 179
access-type	Configures a captive portal's access type	page 180
accounting	Enables a captive portal's accounting records	page 180
bypass	Enables bypassing of captive portal detection requests	page 182
connection-mode	Configures a captive portal's connection mode	page 182
custom-auth	Configures custom user information	page 183
data-limit	Enforces data limit on captive portal clients	page 184
inactivity-timeout	Defines an inactivity timeout in seconds	page 185
logout-fqdn	Clears the logout FQDN address	page 186
no	Reverts the selected captive portal's resets settings to default	*page 4-186*
post-authentication-vlan	Assigns a post authentication RADIUS VLAN for this captive portal's users	page 190
radius-vlan-assignment	Enables an assignment of a RADIUS VLAN for this captive portal	page 191
redirection	Enables redirection of client connections to specified destination ports	page 192
server	Configures the captive portal server settings	page 192
simultaneous-users	Specifies a username used by a MAC address pool	page 194
terms-agreement	Enforces the user to agree to terms and conditions (included in login page) for captive portal access	page 194
use	Associates a AAA policy and a DNS whitelist with a captive portal	page 195
webpage	Configures captive portal Web page settings	page 196

Command	Description	Reference
webpage-auto-upload	Enables automatic upload of advanced Web pages on a captive portal	page 200
webpage-location	Specifies the location of Web pages used for captive portal authentication	page 201
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

access-time

captive-portal-mode commands

Defines the permitted access time for a client. It is used when no session time is defined in the RADIUS response.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
access-time <10-10080>
```

Parameters

```
access-time <10-10080>
```

<10-10080>	Defines the access time allowed for a wireless client from 10 - 10080 minutes. The default is 1440 minutes.

Example

```
rfs7000-37FABE(config-captive-portal-test)#access-time 35

rfs7000-37FABE(config-captive-portal-test)#show context
captive-portal test
 access-time 35
rfs7000-37FABE(config-captive-portal-test)#
```

Related Commands:

no	Reverts to the default permitted access time (1440 minutes)

access-type

captive-portal-mode commands

Defines the captive portal's access type

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
access-type [custom-auth-radius|email|logging|no-auth|radius]
```

Parameters

```
access-type [custom-auth-radius|email|logging|no-auth|radius]
```

custom-auth-radius	Specifies the custom user information used for authentication (RADIUS lookup of given information, such as name, e-mail address, telephone etc.) When selecting this option, use the custom-auth command to configure the required user information.
email	Uses user's e-mail address for authentication
logging	Logs records of users and allowed access. The system logs user access details.
no-auth	Defines no authentication required for a guest (guest is redirected to welcome message). Provides users access to the captive portal without authentication.
radius	Enables RADIUS authentication for wireless clients. Provides captive portal access to successfully authenticated users only. This is the default setting.

Example

```
rfs7000-37FABE(config-captive-portal-test)#access-type logging

rfs7000-37FABE(config-captive-portal-test)#show context
captive-portal test
 access-type logging
 access-time 35
rfs7000-37FABE(config-captive-portal-test)#
```

Related Commands:

no	Removes the captive portal access type or reverts to default (radius)

accounting

captive-portal-mode commands

Enables support for accounting messages for this captive portal

When enabled, accounting for clients entering and exiting the captive portal is initiated. Accounting is the method of collecting and sending security server information for billing, auditing, and reporting user data. This data includes information, such as start and stop times, executed commands (such as PPP), number of packets and number of bytes transmitted etc. Accounting enables tracking of captive portal services consumed by clients.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
accounting [radius|syslog]

accounting radius

accounting syslog host <IP/HOSTNAME> {port <1-65535>} {proxy-mode [none|
          through-controller|through-rf-domain-manager]}
```

Parameters

`accounting radius`

radius	Enables support for RADIUS accounting messages. When enabled, this option uses an external RADIUS resource for AAA accounting. This option is disabled by default.

`accounting syslog host <IP/HOSTNAME> {port <1-65535>} {proxy-mode [none|through-controller|through-rf-domain-manager]}`

syslog host <IP/HOSTNAME>	Enables support for syslog accounting messages. This option is disabled by default. • host <IP/HOSTNAME> – Specifies the destination where accounting messages are sent. Specify the destination's IP address or hostname.
port <1-65535>	Optional. Specifies the syslog server's listener port • <1-65535> – Specify the UDP port from 1- 65535. The default is 514.
proxy-mode [none| through-controller| through-rf-domain-manager]	Optional. Specifies the mode of proxying the syslog server • none – Accounting messages are sent directly to the syslog server • through-controller – Accounting messages are sent through the controller configuring the device • through-rf-domain-manager – Accounting messages are sent through the local RF Domain manager

Example

```
rfs7000-37FABE(config-captive-portal-test)#accounting syslog host
172.16.10.13 port 1

rfs7000-37FABE(config-captive-portal-test)#show context
captive-portal test
 access-type logging
 access-time 35
 accounting syslog host 172.16.10.13 port 1
rfs7000-37FABE(config-captive-portal-test)#
```

Related Commands:

no	Disables accounting records for this captive portal

bypass

captive-portal-mode commands

Enables bypassing of captive portal detection requests from wireless clients

Certain devices, such as Apple IOS devices send *Captive Network Assistant* (CNA) requests to detect existence of captive portals. When enabled, the bypass option does not allow CNA requests to be redirected to the captive portal pages.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
bypass captive-portal-detection
```

Parameters

```
bypass captive-portal-detection
```

bypass captive-portal-detection	Bypasses captive portal detection requests

Example

```
rfs4000-229D58(config-captive-portal-test)#bypass captive-portal-detection

rfs4000-229D58(config-captive-portal-test)#show context
captive-portal test
 bypass captive-portal-detection
rfs4000-229D58(config-captive-portal-test)#
```

Related Commands:

no	Disables bypassing of captive portal detection requests

connection-mode

captive-portal-mode commands

Configures a captive portal's mode of connection to the Web server. HTTP uses plain unsecured connection for user requests. HTTPS uses an encrypted connection to support user requests.

Both HTTP and HTTPS use the same *Uniform Resource Identifier* (URI), so controller and client resources can be identified. However. Brocade recommends the use of HTTPS, as it affords controller and client transmissions some measure of data protection HTTP cannot provide.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
connection-mode [http|https]
```

Parameters

```
connection-mode [http|https]
```

http	Sets HTTP as the default connection mode. This is the default setting.
https	Sets HTTPS as the default connection mode **NOTE:** HTTPS is a more secure version of HTTP, and uses encryption while sending and receiving requests.

Example

```
rfs7000-37FABE(config-captive-portal-test)#connection-mode https

rfs7000-37FABE(config-captive-portal-test)#show context
captive-portal test
 access-type logging
 access-time 35
 connection-mode https
 accounting syslog host 172.16.10.13 port 1
rfs7000-37FABE(config-captive-portal-test)#
```

Related Commands:

no	Removes this captive portal's connection mode

custom-auth

captive-portal-mode commands

Configures custom user information

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
custom-auth info <LINE>
```

Parameters

```
custom-auth info <LINE>
```

info <LINE>	Configures information used for RADIUS lookup when custom-auth RADIUS access type is configured • <LINE> – Guest data needs to be provided. Specify the name, e-mail address, and telephone number of the user.

Example

```
rfs7000-37FABE(config-captive-portal-test)#custom-auth info bob,
bob@motorolasolutions.com

rfs7000-37FABE(config-captive-portal-test)#show context
captive-portal test
 access-type logging
 access-time 35
 custom-auth info bob,\ bob@motorolasolutions.com
 connection-mode https
 accounting syslog host 172.16.10.13 port 1
rfs7000-37FABE(config-captive-portal-test)#
```

Related Commands:

no	Removes custom user information configured with this captive portal

data-limit

captive-portal-mode commands

Enforces data transfer limits on captive portal clients. This feature enables the tracking and logging of user usage. Users exceeding the allowed bandwidth are restricted from the captive portal.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
data-limit <1-102400> {action [log-and-disconnect|log-only]}
```

Parameters

```
data-limit <1-102400> {action [log-and-disconnect|log-only]}
```

data-limit <1-102400>	Sets a captive portal client's data transfer limit in megabytes. This limit is applicable for both upstream and downstream data transfer. • <1-102400> – Specify a value from 1 - 102400 MB.
action [log-and-disconnect| log-only]	Optional. Specifies the action taken when a client exceeds the configured data limit. The options are: • log-and-disconnect – Logs a record and disconnects the client • log-only – Only a log is generated and the client remains connected to the captive portal. This is the default setting.

Example

```
rfs7000-37FABE(config-captive-portal-test)#data-limit 200 action
log-and-disconnect
rfs7000-37FABE(config-captive-portal-test)#

rfs7000-37FABE(config-captive-portal-test)#show context
captive-portal test
 data-limit 200 action log-and-disconnect
rfs7000-37FABE(config-captive-portal-test)#
```

Related Commands:

no	Removes data limit enforcement for captive portal clients

inactivity-timeout

captive-portal-mode commands

Defines an inactivity timeout in seconds. If a frame is not received from a client for the specified interval, the current session is terminated.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
inactivity-timeout <300-86400>
```

Parameters

```
inactivity-timeout <300-86400>
```

<300-86400>	Defines the timeout interval after which a captive portal session is automatically terminated • <300-86400> – Specify a value from 300 - 86400 seconds. The default is 10 minutes or 600 seconds.

Example

```
rfs7000-37FABE(config-captive-portal-test)#inactivity-timeout 750

rfs7000-37FABE(config-captive-portal-test)#show context
captive-portal test
 access-type logging
 access-time 35
 custom-auth info bob,\ bob@motorolasolutions.com
 connection-mode https
 inactivity-timeout 750
 accounting syslog host 172.16.10.13 port 1
rfs7000-37FABE(config-captive-portal-test)#
```

Related Commands:

no	Removes the client inactivity interval configured with this captive portal

logout-fqdn

captive-portal-mode commands

Configures the *Fully Qualified Domain Name* (FQDN) address to logout of the session from the client

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
logout-fqdn <WORD>
```

Parameters

```
logout-fqdn <WORD>
```

logout-fqdn <WORD>	Configures the FQDN address used to logout • <WORD> – Provide the FQDN address (for example, logout.guestaccess.com).

Example

```
rfs7000-37FABE(config-captive-portal-test)#logout-fqdn logout.testuser.com
rfs7000-37FABE(config-captive-portal-test)#

rfs7000-37FABE(config-captive-portal-test)#show context
captive-portal test
 logout-fqdn logout.testuser.com
rfs7000-37FABE(config-captive-portal-test)#
```

Related Commands:

no	Clears the logout FQDN address

no

captive-portal-mode commands

The no command reverts the selected captive portal's resets settings to default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no
[access-time|access-type|accounting|bypass|connection-mode|custom-auth|data-l
imit|

inactivity-timeout|logout-fqdn|post-authentication-vlan|radius-vlan-assignmen
t|
          redirection|server|simultaneous-users|terms-agreement|use|webpage|
          webpage-auto-upload|webpage-location]

no [access-time|access-type|connection-mode|data-limit|inactivity-timeout|

logout-fqdn|post-authentication-vlan|radius-vlan-assignment|simultaneous-user
s|
          terms-agreement|webpage-auto-upload|webpage-location]

no accounting [radius|syslog]

no bypass captive-portal-detection

no custom-auth info

no redirection ports

no server host
no server mode {centralized-controller [hosting-vlan-interface]}

no use [aaa-policy|dns-whitelist]

no webpage external [acknowledgment|agreement|fail|login
{post}|no-service|welcome]

no webpage internal [org-name|org-signature]
no webpage internal [acknowledgment|agreement|fail|login|no-service|welcome]
          [description|footer|header|main-logo|small-logo|title]
```

Parameters

```
no [access-time|access-type|connection-mode|data-limit|inactivity-timeout|
logout-fqdn|post-authentication-vlan|radius-vlan-assignment|simultaneous-user
s|
terms-agreement|webpage-auto-upload|webpage-location]
```

no access-time	Resets client access time
no access-type	Resets client access type
no connection-mode	Resets connection mode to HTTP
no data-limit	Removes data limit enforcement for captive portal clients
no inactivity-timeout	Resets inactivity timeout interval
no logout-fqdn	Clears the logout FQDN address
no post-authentication-vlan	Removes the post authentication RADIUS VLAN assigned to this captive portal's users
no radius-vlan-assignment	Disables RADIUS VLAN assignment for captive portal users
no simultaneous-users	Resets the number of MAC addresses that can use a single user name to its default of 1
no terms-agreement	Resets the terms of agreement required for logging in. The user no longer has to agree to terms & conditions before connecting to a captive portal.

no webpage-auto-upload	Disables automatic upload of advanced Web pages on a captive portal
no webpage-location	Resets the use of custom Web pages for login, welcome, terms, and failure page. The default is automatically created Web pages.

`no accounting [radius|syslog]`

no accounting	Disables accounting configurations
radius	Disables support for sending RADIUS accounting messages
syslog	Disables support for sending syslog messages to remote syslog servers

`no bypass captive-portal-detection`

no bypass captive-portal-detection	Disables bypassing of captive-portal detection requests

`no custom-auth info`

no custom-auth	Resets custom authentication information
info	Resets the configuration of custom user information sent to the RADIUS server (for custom-auth-radius access type)

`no redirection ports`

no redirection ports	Disables redirection of client connections to specified destination ports

`no server host`

no server host	Clears captive portal server address

`no server mode` *`{centralized-controller [hosting-vlan-interface]}`*

no server mode	Configures the captive portal server mode
centralized-controller hosting-vlan-interface	Optional. Resets the hosting VLAN interface for centralized captive portal server to its default of zero (0)

`no use [aaa-policy|dns-whitelist]`

no use	Resets profiles used with a captive portal policy
aaa-policy	Removes the AAA policy used with a captive portal policy
dns-whitelist	Removes the DNS whitelist used with a captive portal policy

`no webpage external [acknowledgment|agreement|fail|login` *`{post}`*`|no-service|welcome]`

no webpage external	Resets the external Web pages settings. These are the Web pages (externally located) displayed when a user interacts with the captive portal.
acknowledgment	Resets the acknowledgment page location
agreement	Resets the agreement page settings
fail	Resets the fail page settings
login {post}	Resets the login page settings • post – Optional. Users are redirected to post internally when they try to authenticate

no-service	Resets the no-service page settings. The no-service Web page is displayed when critical services (such as, AAA server, captive portal server, DHCP server, and AP to controller connectivity) are not reachable and the user cannot access the captive portal.
welcome	Resets the welcome page settings

```
no webpage internal [org-name|org-signature]
```

no webpage internal	Resets the configuration of internal Web pages displayed when a user interacts with the captive portal
org-name	Resets the organization name that is included at the top of Web pages
org-signature	Resets the organization signature (email, addresses, phone numbers) included at the bottom of Web pages

```
no webpage internal [acknowledgment|agreement|fail|login|no-service|welcome]
[description|footer|header|main-logo|small-logo|title]
```

no webpage internal	Resets the of internal Web pages settings. These are the Webpages (internally located) displayed when a user interacts with the captive portal.
acknowledgment	Resets the acknowledgment page settings
agreement	Resets the agreement page settings
fail	Resets the fail page settings
login	Resets the login page settings
no-service	Resets the no-service page settings. The no-service Web page is displayed when critical services (such as, AAA server, captive portal server, DHCP server) are not reachable and the user cannot access the captive portal.
welcome	Resets the welcome page settings
description	Resets the description part of each Web page. This is the area where information about the captive portal and user state is displayed to the user.
footer	Resets the footer portion of each Web page. A footer can contain the organization signature
header	Resets the header portion of each Web page
main-logo	Resets the main logo of each Web page
small-logo	Resets the small logo of each Web page
title	Resets the title of each Web page

Example

```
The following example shows the captive portal ‘test’ settings before the ‘no’
commands are executed:

rfs7000-37FABE(config-captive-portal-test)#show context
captive-portal test
 access-type logging
 access-time 35
 custom-auth info bob,\ bob@motorolasolutions.com
 connection-mode https
 inactivity-timeout 750
 accounting syslog host 172.16.10.13 port 1
rfs7000-37FABE(config-captive-portal-test)#

rfs7000-37FABE(config-captive-portal-test)#no accounting syslog
rfs7000-37FABE(config-captive-portal-test)#no access-type
```

```
The following example shows the captive portal ‘test’ settings after the ‘no’
commands are executed:

rfs7000-37FABE(config-captive-portal-test)#show context
captive-portal test
 access-time 35
 custom-auth info bob,\ bob@motorolasolutions.com
 connection-mode https
 inactivity-timeout 750
rfs7000-37FABE(config-captive-portal-test)#
```

Related Commands:

access-time	Configures the allowed access time for each captive portal client
access-type	Configures captive portal authentication and logging information
accounting	Configures captive portal accounting information
bypass	Enables bypassing of captive portal detection requests
connection-mode	Configures how clients connect to a captive portal
custom-auth	Configures the captive portal parameters required for client access
inactivity-timeout	Configures the client inactivity timeout interval
logout-fqdn	Configures the FQDN address to logout of the session from the client
post-authentication-vlan	Assigns a post authentication RADIUS VLAN for this captive portal’s users
radius-vlan-assignment	Enables assignment of a RADIUS VLAN for this captive portal
redirection	Enables redirection of client connections to specified destination ports
server	Configures captive portal server parameters
simultaneous-users	Configures the maximum number of clients that can use a single captive portal user name
terms-agreement	Configures if a client has to accept terms and conditions before logging to the captive portal
use	Associates a AAA policy and DNS whitelist with this captive portal policy
webpage-location	Configures the location of Web pages displayed when the user interacts with the captive portal
webpage	Configures Web pages used by the captive portal to interact with users
webpage-auto-upload	Enables automatic upload of advanced Web pages on a captive portal
aaa-policy	Configures a AAA policy
dns-whitelist	Configures a DNS whitelist

post-authentication-vlan

captive-portal-mode commands

Assigns a post authentication RADIUS VLAN for this captive portal’s users

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
post-authentication-vlan <1-4096>
```

Parameters

```
post-authentication-vlan <1-4096>
```

post-authentication-vlan <1-4096>	Assigns a VLAN for this captive portal's users after they have authenticated and logged on to the network • <1-4096> – Specify the VLAN's number from 1 - 4096.

Example

```
rfs4000-229D58(config-captive-portal-test)#post-authentication-vlan 1
rfs4000-229D58(config-captive-portal-test)#

rfs4000-229D58(config-captive-portal-test)#show context
captive-portal test
 post-authentication-vlan 1
rfs4000-229D58(config-captive-portal-test)#
```

Related Commands:

no	Removes the post authentication RADIUS VLAN assigned to this captive portal's users
radius-vlan-assignment	Enables assignment of a RADIUS VLAN for this captive portal

radius-vlan-assignment

captive-portal-mode commands

Enables assignment of a RADIUS VLAN for this captive portal

When enabled, if the RADIUS server as part of the authentication process returns a client's VLAN-ID in a RADIUS access-accept packet, then all client traffic is forwarded on the post authentication VLAN. If disabled, the RADIUS server's VLAN assignment is ignored and the VLAN configuration defined within the WLAN configuration is used instead. This feature is disabled by default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
radius-vlan-assignment
```

Parameters

None

Example

```
rfs4000-229D58(config-captive-portal-test)#radius-vlan-assignment
rfs4000-229D58(config-captive-portal-test)#
```

```
rfs4000-229D58(config-captive-portal-test)#show context
captive-portal test
 post-authentication-vlan 1
 radius-vlan-assignment
rfs4000-229D58(config-captive-portal-test)#
```

Related Commands:

no	Disables assignment of a RADIUS VLAN for this captive portal
post-authentication-vlan	Assigns a post authentication RADIUS VLAN for this captive portal's users

redirection

captive-portal-mode commands

Enables redirection of client connections to specified destination ports

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
redirection ports <LIST-OF-PORTS>
```

Parameters

```
redirection ports <LIST-OF-PORTS>
```

ports <LIST-OF-PORTS>	Configures destination ports considered for redirecting client connection

Example

```
rfs4000-229D58(config-captive-portal-test)#redirection ports 1,2,3
rfs4000-229D58(config-captive-portal-test)#

rfs4000-229D58(config-captive-portal-test)#show context
captive-portal test
 redirection ports 1-3
rfs4000-229D58(config-captive-portal-test)#
```

Related Commands:

no	Disables redirection of client connection

server

captive-portal-mode commands

Configures captive portal server parameters, such as the hostname, IP, and mode of operation

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
server [host|mode]
server host <IP/HOSTNAME>
server mode [centralized|centralized-controller {hosting-vlan-interface
<0-4096>}|
          self]
```

Parameters

`server host <IP/HOSTNAME>`

host <IP/HOSTNAME>	Configures the internal captive portal authentication server (wireless controller, access point, service platform) • <IP/HOSTNAME> – Specify the IP address or hostname of the captive portal server. **NOTE:** For centralized wireless controller mode, this should be a virtual hostname and not IP address.

`server mode [centralized|centralized-controller {hosting-vlan-interface <0-4096>}| self]`

mode	Configures the captive portal server mode
centralized	Considers the configured server's hostname or IP address as the centralized captive portal server. Select this option if the captive portal is supported on an external server.
centralized-controller {hosting-vlan-interface <0-4096>}	Configures the numeric IP address (or DNS hostname) for the server validating guest user permissions for the captive portal policy. This option is available only for the *centralized* (external) AND *centralized-controller captive portal* server resources. • hosting-vlan-interface – Optional. Configures the VLAN where the client can reach the wireless controller (server). This option is available only for the centralized-controller mode. • <0-4096> – Specify the VLAN number (0 implies the controller is available on the client's VLAN).
self	Selects the captive portal server as the same device supporting the WLAN (the captive portal and the WLAN are configured on the same device). Select this option to maintain the captive portal configuration (Web pages) internally. This is the default setting.

Example

```
rfs7000-37FABE(config-captive-portal-test)#server host 172.16.10.9

rfs7000-37FABE(config-captive-portal-test)#show context
captive-portal test
 access-time 35
 custom-auth info bob,\ bob@motorolasolutions.com
 connection-mode https
 inactivity-timeout 750
 server host 172.16.10.9
rfs7000-37FABE(config-captive-portal-test)#
```

Related Commands:

no	Resets or disables captive portal host and mode settings

simultaneous-users

captive-portal-mode commands

Specifies the number of MAC addresses that can simultaneously use a particular username. This option is disabled by default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
simultaneous-users <1-8192>
```

Parameters

```
simultaneous-users <1-8192>
```

<1-8192>	Specifies the number of MAC addresses that can simultaneously use a particular username. Select a number from 1 - 8192.

Example

```
rfs7000-37FABE(config-captive-portal-test)#simultaneous-users 5

rfs7000-37FABE(config-captive-portal-test)#show context
captive-portal test
 access-time 35
 custom-auth info bob,\ bob@motorolasolutions.com
 connection-mode https
 inactivity-timeout 750
 server host 172.16.10.9
 simultaneous-users 5
rfs7000-37FABE(config-captive-portal-test)#
```

Related Commands:

no	Resets or disables captive portal commands

terms-agreement

captive-portal-mode commands

Enforces the user to agree to terms and conditions (included in the login page) for captive portal access. This feature is disabled by default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
terms-agreement
```

Parameters

None

Example

```
rfs7000-37FABE(config-captive-portal-test)#terms-agreement

rfs7000-37FABE(config-captive-portal-test)#show context
captive-portal test
 access-time 35
 custom-auth info bob,\ bob@motorolasolutions.com
 connection-mode https
 inactivity-timeout 750
 server host 172.16.10.9
 simultaneous-users 5
 terms-agreement
rfs7000-37FABE(config-captive-portal-test)#
```

Related Commands:

no	Resets or disables captive portal commands

use

captive-portal-mode commands

Configures a AAA policy and DNS whitelist with this captive portal policy. AAA policies are used to configure authentication and accounting servers for this captive portal. DNS whitelists restrict users to a set of configurable domains on the Internet.

For more information on AAA policies, see *Chapter 8, AAA-POLICY*.

For more information on DNS whitelists, see *Chapter 4, dns-whitelist.*

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
use [aaa-policy <AAA-POLICY-NAME>|dns-whitelist <DNS-WHITELIST-NAME>]
```

Parameters

```
use [aaa-policy <AAA-POLICY-NAME>|dns-whitelist <DNS-WHITELIST-NAME>]
```

aaa-policy <AAA-POLICY-NAME>	Configures a AAA policy with this captive portal. AAA policies validate user credentials and provide captive portal access to the network. • <AAA-POLICY-NAME> – Specify the AAA policy name.
dns-whitelist <DNS-WHITELIST-NAME>	Configures a DNS whitelist to use with this captive portal. DNS whitelists restrict captive portal access. • <DNS-WHITELIST-NAME> – Specify the DNS whitelist name. To effectively host captive portal pages on an external Web server, the IP address of the destination Web server(s) should be added to the DNS whitelist.

Example

```
rfs7000-37FABE(config-captive-portal-test)#use aaa-policy test

rfs7000-37FABE(config-captive-portal-test)#use dns-whitelist test

rfs7000-37FABE(config-captive-portal-test)#show context
captive-portal test
 access-time 35
 custom-auth info bob,\ bob@motorolasolutions.com
 connection-mode https
 inactivity-timeout 750
 server host 172.16.10.9
 simultaneous-users 5
 terms-agreement
 use aaa-policy test
 use dns-whitelist test
rfs7000-37FABE(config-captive-portal-test)#
```

Related Commands:

no	Removes a DNS Whitelist or a AAA policy from the captive portal
dns-whitelist	Configures a DNS whitelist
aaa-policy	Configures a AAA policy

webpage

captive-portal-mode commands

Use this command to define the appearance and flow of Web pages requesting clients encounter when accessing a controller, service platform, or access point managed captive portal. Define whether the Web pages are maintained locally or externally to the managing device as well as messages displayed requesting clients.

Configures Web pages displayed when interacting with a captive portal. There are six (6) different pages.

- acknowledgment – This page displays details for the user to acknowledge
- agreement – This page displays “Terms and Conditions” that a user accepts before allowed access to the captive portal.
- fail – This page is displayed when the user is not authenticated.
- login – This page is displayed when the user connects to the captive portal. It fetches login credentials from the user.
- no-service – This page is displayed when a captive portal user is unable to access the captive portal due unavailability of critical services.

- welcome – This page is displayed to welcome an authenticated user to the captive portal.

These Web pages, which interact with captive portal users, can be located either on the controller or an external location.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
webpage [external|internal]

webpage external [acknowledgment|agreement|fail|login
{post}|no-service|welcome]
          <URL>

webpage internal [acknowledgment|agreement|fail|login|no-service|org-name|
          org-signature|welcome]

webpage internal [acknowledgment|agreement|fail|login|no-service|welcome]
          [description|footer|header|title] <CONTENT>

webpage internal [acknowledgment|agreement|fail|login|no-service|welcome]
          [main-logo|small-logo] <URL>

webpage internal [org-name|org-signature] <LINE>
```

Parameters

```
webpage external [acknowledgment|agreement|fail|login
{post}|no-service|welcome] <URL>
```

external	Indicates Web pages being served are hosted on an external (to the captive portal) server resource
acknowledgment	Indicates the page is displayed for user acknowledgment of details. Users are redirected to this page to acknowledge information provided.
agreement	Indicates the page is displayed for “Terms & Conditions” The agreement page provides conditions that must be agreed to before captive portal access is permitted.
fail	Indicates the page is displayed for login failure The fail page asserts authentication attempt has failed, the user is not allowed to access the Internet (using this captive portal) and must provide the correct login information again to access the Internet.
login {post}	Indicates the page is displayed for getting user credentials. This page is displayed by default. • post – Optional. Redirects users to post externally when they during authentication The login page prompts the user for a username and password to access the captive portal and proceed to either the agreement page (if used) or the welcome page.

no-service	Indicates the page is displayed when certain critical services are unavailable and the user fails to access the captive portal. The no-service page asserts the captive portal service is temporarily unavailable due to technical reasons. Once the services become available, the captive portal user is automatically connected back to the services available through the captive portal. The possible scenarios are: • The RADIUS server (on-board or external) is not reachable and the user cannot be authenticated • The external captive portal server is not reachable • The connectivity between the adopted AP and controller is lost • The external DHCP server is not reachable To provide this service, enable the following: • External captive portal server monitoring • AAA server monitoring. This enables detection of RADIUS server failure. • External DHCP server monitoring For more information on enabling these critical resource monitoring, see *Chapter 4, service*.
welcome	Indicates the page is displayed after a user has been successfully authenticated The welcome page asserts a user has logged in successfully and can access the captive portal.
<URL>	Indicates the URL to the Web page displayed. Query String: URL can include query tags. Supported Query Tags are: 'WING_TAG_CLIENT_IP' - Captive portal client IPv4 address 'WING_TAG_CLIENT_MAC' - Captive portal client MAC address 'WING_TAG_WLAN_SSID ' - Captive portal client WLAN ssid 'WING_TAG_AP_MAC' - Captive portal client AP MAC address 'WING_TAG_AP_NAME' - Captive portal client AP Name 'WING_TAG_RF_DOMAIN' - Captive portal client RF Domain 'WING_TAG_CP_SERVER' - Captive portal server address 'WING_TAG_USERNAME' - Captive portal authentication username Example: http://cportal.com/policy/login.html?client_ip=WING_TAG_CLIENT_IP&ap_m c=WING_TAG_AP_MAC. Use '&' or '?' character to separate field-value pair. Note: Enter 'ctrl-v' followed by '?' to configure query string

```
webpage internal [acknowledgment|agreement|fail|login|no-service|welcome]
[description|footer|header|title] <CONTENT>
```

internal	Indicates the Web pages are internal. This is the default setting.
acknowledgment	Indicates the Web page is displayed for users to acknowledge the information provided
agreement	Indicates the page is displayed for “Terms & Conditions”
fail	Indicates the page is displayed for login failure
login	Indicates the page is displayed for user credentials
no-service	Indicates the page is displayed when certain critical services are unavailable and the user fails to access the captive portal. The possible scenarios are: • The RADIUS server (on-board or external) is not reachable and the user cannot be authenticated • The external captive portal server is not reachable • The connectivity between the adopted AP and controller is lost • The external DHCP server is not reachable To provide this service, enable the following: • External captive portal server monitoring • AAA server monitoring. This enables detection of RADIUS server failure. • External DHCP server monitoring • AP to controller connectivity monitoring For more information on enabling these critical resource monitoring, see *Chapter 4, service*.
welcome	Indicates the page is displayed after a user has been successfully authenticated

description	Indicates the content is the description portion of each of the following internal Web pages: acknowledgment, agreement, fail, login, no-service, and welcome
footer	Indicates the content is the footer portion of each of the following internal Web pages: acknowledgment, agreement, fail, no-service, and welcome page. The footer portion contains the signature of the organization that hosts the captive portal.
header	Indicates the content is the header portion of each of the following internal Web pages: acknowledgment, agreement, fail, no-service, and welcome page. The header portion contains the heading information for each of these pages.
title	Indicates the content is the title of each of the following internal Web pages: acknowledgment, agreement, fail, no-service, and welcome page. The title for each of these pages is configured here.
<CONTENT>	The following keyword is common to all of the above internal Web page options: • <CONTENT> – Specify the content displayed for each of the different components of the internal Web page. Enter up to 900 characters for the description and 256 characters each for header, footer, and title.
	`webpage internal [acknowledgment|agreement|fail|login|no-service|welcome] [main-logo|small-logo] <URL>`
internal	Indicates the Web pages are internal
agreement	Indicates the page is displayed for “Terms & Conditions”
acknowledgment	Indicates the Web page is displayed for users to acknowledge the information provided
fail	Indicates the page is displayed for login failure
login	Indicates the page is displayed for user credentials
no-service	Indicates the page is displayed when certain critical services are unavailable and the user fails to access the captive portal. The possible scenarios are: • The RADIUS server (on-board or external) is not reachable and the user cannot be authenticated • The external captive portal server is not reachable • The connectivity between the adopted AP and controller is lost • The external DHCP server is not reachable To provide this service, enable the following: • External captive portal server monitoring • AAA server monitoring. This enables detection of RADIUS server failure. • External DHCP server monitoring • AP to controller connectivity monitoring For more information on enabling these critical resource monitoring, see *wlan*.
welcome	Indicates the page is displayed after a user has been successfully authenticated
main-logo	The following keyword is common to all of the above internal Web page options: • main-logo – Indicates the main logo displayed in the header portion of each Web page
small-logo	The following keyword is common to all of the above internal Web page options: • small-logo – Indicates the logo image displayed in the footer portion of each Web page, and constitutes the organization’s signature
<URL>	Provides the complete URL of the main-logo and small-logo files • <URL> – Specify the location of the main-logo and the small-logo files. The files are loaded from the specified location.
	`webpage internal [org-name|org-signature] <LINE>`
internal	Indicates the Web pages are internal
org-name	Specifies the company’s name, included on Web pages along with the main image

org-signature	Specifies the company's signature information, included in the bottom of Web pages along with a small image
<LINE>	Specify the company's name or signature depending on the option selected.

Example

```
rfs7000-37FABE(config-captive-portal-test)#webpage external fail
http://www.motorolasolutions.com

rfs7000-37FABE(config-captive-portal-test)#show context
captive-portal test
 access-time 35
 custom-auth info bob,\ bob@motorolasolutions.com
 connection-mode https
 inactivity-timeout 750
 server host 172.16.10.9
 simultaneous-users 5
 terms-agreement
 webpage-location external
 webpage external fail http://www.motorolasolutions.com
 use aaa-policy test
rfs7000-37FABE(config-captive-portal-test)#
```

Related Commands:

no	Resets or disables captive portal configurations

webpage-auto-upload

captive-portal-mode commands

Enables automatic upload of advanced Web pages on a captive portal. Enable this option if the webpage-location is selected as *advanced*. For more information see, *webpage-location*.

If this feature is enabled, access points shall request for Web pages from the controller during adoption. If the controller has a different set of Web pages, than the ones existing on the access points, the controller shall distribute the Web pages uploaded on it to the access points.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
webpage-auto-upload
```

Parameters

None

Example

```
rfs7000-37FABE(config-captive-portal-test)#webpage-auto-upload
rfs7000-37FABE(config-captive-portal-test)#
```

```
rfs7000-37FABE(config-captive-portal-test)#show context
captive-portal test
 webpage-auto-upload
 logout-fqdn logout.testuser.com
rfs7000-37FABE(config-captive-portal-test)#
```

Related Commands:

no	Disables automatic upload of advanced Web pages on a captive portal
webpage	Configures Web pages displayed when interacting with a captive portal
webpage-location	Specifies the location of the Web pages used for authentication

webpage-location

captive-portal-mode commands

Specifies the location of the Web pages used for authentication. These pages can either be hosted on the system or on an external Web server.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
webpage-location [advanced|external|internal]
```

Parameters

```
webpage-location [advanced|external|internal]
```

advanced	Uses Web pages for login, welcome, failure, and terms created and stored on the controller. Select *advanced* to use a custom-developed directory full of Web page content that can be copied in and out of the controller, service platform, or access point. If selecting advanced, enable the *webpage-auto-upload* option to automatically launch the advanced pages to requesting clients upon association. For more information, see *webpage-auto-upload*.
external	Uses Web pages for login, welcome, failure, and terms located on an external server. Provide the URL for each of these pages.
internal	Uses Web pages for login, welcome, and failure that are automatically generated

Example

```
rfs7000-37FABE(config-captive-portal-test)#webpage-location external

rfs7000-37FABE(config-captive-portal-test)#show context
captive-portal test
 access-time 35
 custom-auth info bob,\ bob@motorolasolutions.com
 connection-mode https
 inactivity-timeout 750
```

```
 server host 172.16.10.9
 simultaneous-users 5
 terms-agreement
 webpage-location external
 use aaa-policy test
rfs7000-37FABE(config-captive-portal-test)#
```

Related Commands:

no	Resets or disables captive portal Web page settings
webpage	Configures a captive portal's Web page (acknowledgment, agreement, login, welcome, fail, no-service, and terms) settings
webpage-auto-upload	Enables an automatic upload of advanced Web pages on a captive portal

clear

Global Configuration Commands

Clears parameters, cache entries, table entries, and other similar entries. The clear command is available for specific commands only. The information cleared using this command varies depending on the mode where executed.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
clear event-history
```

Parameters

```
clear event-history
```

event-history	Clears the event history file

Example

```
rfs4000-229D58#show event-history
EVENT HISTORY REPORT
Generated on '2013-01-31 00:15:57 UTC' by 'admin'

2013-01-31 00:15:36     rfs4000-229D58  SYSTEM     LOGIN
Successfully logged in user 'admin' with privilege 'superuser' from 'ssh'
2013-01-30 23:43:10  rfs4000-229D58 SYSTEM  UI_USER_AUTH_SUCCESS UI user
'admin' from: '192.168.100.224' authentication successful
2013-01-30 03:47:47     rfs4000-229D58  SYSTEM     LOGOUT              Logged
out user 'admin' with privilege 'superuser' from '192.168.100.231(web)'
2013-01-30 02:45:08  rfs4000-229D58 SYSTEM  UI_USER_AUTH_SUCCESS UI user
'admin' from: '192.168.100.231' authentication successful
2013-01-28 20:28:29     rfs4000-229D58  SYSTEM     LOGOUT              Logged
out user 'admin' with privilege 'superuser' from '192.168.100.173(web)'
```

```
2013-01-28 19:56:31  rfs4000-229D58 SYSTEM  UI_USER_AUTH_SUCCESS UI user
'admin' from: '192.168.100.173' authentication successful
2013-01-27 20:15:20     rfs4000-229D58  SYSTEM     LOGOUT              Logged
out user 'admin' with privilege 'superuser' from '192.168.100.204'
2013-01-27 20:14:45     rfs4000-229D58  SYSTEM     LOGIN
Successfully logged in user 'admin' with privilege 'superuser' from 'ssh'
2013-01-27 19:53:25     rfs4000-229D58  SYSTEM     LOGOUT              Logged
out user 'admin' with privilege 'superuser' from '192.168.100.204'
2013-01-27 19:43:22     rfs4000-229D58  SYSTEM     LOGIN
Successfully logged in user 'admin' with privilege 'superuser' from 'ssh'
--More--
rfs4000-229D58#

rfs4000-229D58#clear event-history
rfs4000-229D58#

rfs4000-229D58#show event-history
EVENT HISTORY REPORT
Generated on '2013-02-15 14:59:21 UTC' by 'admin'

2013-02-15 14:44:19     rfs4000-229D58  SYSTEM     CLOCK_RESET         System
clock reset, Time: 2013-02-15 14:45:30
rfs4000-229D58#
```

client-identity

Global Configuration Commands

With an increase in *Bring Your Own Device* (BYOD) corporate networks, there is a parallel increase in the number of possible attack scenarios within the network. BYOD devices are inherently unsafe, as the organization's security mechanisms do not extend to these personal devices deployed in the corporate wireless network. Organizations can protect their network by limiting how and what these BYODs can access on and through the corporate network.

Device fingerprinting assists administrators by controlling how BYOD devices access a corporate wireless domain.

Device fingerprinting uses DHCP options sent by the client in request or discover packets to derive a unique signature specific to device class. For example, Apple devices have a different signature from Android devices. The signature is used to classify the devices and assign permissions and restrictions on each device class.

The following table summarizes the commands available for creating and configuring a set of new client identity parameters.

Command	Description	Reference
client-identity	Creates a new client identity and enters its configuration mode	page 203
client-identity-mode commands	Invokes the client identity policy configuration mode commands	page 205
client-identity-group	Creates a new client identity group and enters its configuration mode	page 209

client-identity

client-identity

Creates a new client identity and enters its configuration mode. Client identity is a set of unique fingerprints used to identify a class of devices. This information is used to configure permissions and access rules for the identified class of devices in the network. The client-identity feature enables device fingerprinting.

Device fingerprinting is a technique of collecting, analyzing, and identifying traffic patterns originating from remote computing devices. When enabled, device fingerprinting helps to identify a wireless client's device type. There are two methods of fingerprinting devices: Active and Passive.

Active fingerprinting is based on the fact that traffic patterns vary with varying device types. It involves the sending of requests (HTTP etc.) to devices (clients) and analyzing their response to determine the device type. For example, an invalid request is sent to a device, and its error response is analyzed to identify the device type. Since active device fingerprinting involves sending of packets, the probability of the network getting flooded is very high, especially when many devices are being fingerprinted simultaneously.

Passive fingerprinting involves monitoring of devices to check for known traffic patterns specific to devices based on the protocol, driver implementation etc. This method accurately classifies a client's TCP/IP configuration, OS fingerprints, wireless settings etc. No packets are sent to the device. Some of the commonly used protocols for passive device fingerprinting are, TCP, DHCP, HTTP etc.

This feature implements DHCP device fingerprinting, which relies on specific information sent by a wireless client when acquiring IP address and other configuration information from a DHCP server. The feature uses the DHCP options sent by the wireless client in the DHCP request or discover packets to derive a unique signature specific to the class of devices. For example, Apple devices have a different signature than Android devices. This unique signature can then be used to classify the devices and assign permissions and restrictions on each device class.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
client-identity <CLIENT-IDENTITY-NAME>
```

Parameters

```
client-identity <CLIENT-IDENTITY-NAME>
```

client-identity <CLIENT-IDENTITY–NAME>	Creates a new client identity policy and enters its configuration mode • <CLIENT-IDENTITY–NAME> – Specify a client identity policy name. If the client identity policy does not exist, it is created.

Usage Guidelines:

The following points should be considered when configuring the client identity (device fingerprinting) feature:

1. Ensure that DHCP is enforced on the WLANs. For more information on enforcing DHCP on WLANs, see *enforce-dhcp*.

2. Successful identification of different device types depends on the uniqueness of the configured fingerprints. DHCP fingerprinting identifies clients based on the patterns (fingerprints) in the DHCP discover and request messages sent by clients. If different operating systems have the same fingerprints. it will be difficult to identity the device type.
3. When associating client identities with a role policy, ensure that the profile/device, under which the role policy is being used, also has an associated client identity group (containing all the client identities used by the role policy).

Example

```
rfs4000-229D58(config)#client-identity test
rfs4000-229D58(config-client-identity-test)#?

rfs4000-229D58(config-client-identity-test)#?
Client Identity Mode commands:
  dhcp                      Add a DHCP option based match criteria
  dhcp-match-message-type   Specify DHCP message type to match
  no                        Negate a command or set its defaults

  clrscr                    Clears the display screen
  commit                    Commit all changes made in this session
  do                        Run commands from Exec mode
  end                       End current mode and change to EXEC mode
  exit                      End current mode and down to previous mode
  help                      Description of the interactive help system
  revert                    Revert changes
  service                   Service Commands
  show                      Show running system information
  write                     Write running configuration to memory or terminal

rfs4000-229D58(config-client-identity-test)#
```

client-identity-mode commands

client-identity

The following table summarizes a new client's identity configuration mode commands.

Command	Description	Reference
dhcp	Configures the DHCP option match criteria for device fingerprinting	page 205
dhcp-match-message-type	Configures the DHCP message type for device fingerprinting	page 207
no	Removes the DHCP option (used for client identification) configurations	page 208

dhcp

client-identity-mode commands

Configures the DHCP option match criteria (signature) for the discover and request message types received from wireless clients

When accessing a network, DHCP discover and request messages are passed between wireless clients and the DHCP server. These messages contain DHCP options and option values that differ from device to device and are based on the DHCP implementation in the device's *operating system* (OS). Options and option values contained in a client's messages are parsed and compared against the configured DHCP option values to identify the device. Once a device type is identified, the wireless client database is updated with the discovered device type.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
dhcp <1-16> [message-type|option|option-modes]

dhcp <1-16> message-type [discover|request] [option|option-codes]
dhcp <1-16> message-type [discover|request] [option <1-254>|option-codes]
          [contains|exact|starts-with] [ascii|hexstring] <WORD>
```

Parameters

```
dhcp <1-16> message-type [discover|request] [option <1-254>|option-codes]
       [contains|exact|starts-with] [ascii|hexstring] <WORD>
```

dhcp <1-16>	Adds a DHCP option match criteria signature • <1-16> – Specify an index for this DHCP match criteria from 1 - 16. A maximum of 16 match criteria can be configured.
message-type [discover|request]	Specifies the message type to which this DHCP match criteria is applicable • discover – Applies this match criteria to DHCP discover messages only. Indicates that the fingerprint is only checked with any DHCP discover messages received from any device. • request – Applies this match criteria to DHCP request messages only. Indicates that the fingerprint is only checked with any DHCP request messages received from any device. It is recommended to configure client-identity with request messages, because clients rarely send discover messages. If the message type is not specified, the fingerprint is checked with all message types (DHCP request and DHCP discover)
option <1-254>	The following keywords are common to the 'discover' and 'request' message types: • option – Configures a DHCP option value, which is used as the match criteria • <1-254> – Configures a code for this DHCP option from 1 - 254 (except option 53)
option-codes	The following keyword is common to the 'discover' and 'request' message types: • option-codes – Matches criteria based on the DHCP option codes contained in the client's discover/request messages Devices pass options in their DHCP discover/request messages as option codes, option types, and option value sets. These option codes are extracted and matched against the configured DHCP option codes and a fingerprint is derived. This derived fingerprint is used to identify the device.
contains	The following keyword is common to the 'discover' and 'request' message types: • contains – Specifies that the DHCP options received in the client's discover/request messages contains the configured option code string

exact	The following keyword is common to the discover and request message types: • exact – Specifies that the DHCP options received in the client's discover/request messages is an exact match with the configured option code string
starts-with	The following keyword is common to the 'discover' and 'request' message types: • starts-with – Specifies that the DHCP options received in the client's discover/request messages starts with the configured option code string
ascii <WORD>	The following keywords are common to the 'contains', 'exact', and 'starts-with' parameters: • ascii – Configures the DHCP option in the ASCII format • <WORD> – Specify the DHCP option ASCII value to match.
hexstring <WORD>	The following keywords are common to the 'contains', 'exact', and 'starts-with' parameters: • hexstring – Configures the DHCP option in the hexa-decimal format • <WORD> – Specify the DHCP option hexstring value to match.

Usage Guidelines:

The following DHCP options are useful for identifying different device types:

1. Option 55: Used by a DHCP client to request values for specific configuration parameters. It is a list of DHCP option codes and can be in the client's order of preference.
2. Client configured list of DHCP options (all options parsed into a hex string).
3. Option 60: Vendor class identifier. Used to identify the vendor and functionality of a DHCP client (some devices do not set the value of this field).

Though it is possible to use any option to configure a device fingerprint, Brocade recommends the use of a combination of one or more of the preceding options to define a device.

Example

```
rfs4000-229D58(config-client-identity-test)#dhcp 1 message-type request option
60 exact ascii MSFT\5.0
rfs4000-229D58(config-client-identity-test)#dhcp 2 message-type discover
option
 2 exact hexstring 012456c22c44


rfs4000-229D58(config-client-identity-test)#show context
client-identity test
 dhcp 2 message-type discover option 2 exact hexstring 012456c22c44
 dhcp 1 message-type request option 60 exact ascii MSFT5.0
rfs4000-229D58(config-client-identity-test)#
```

Related Commands:

no	Removes a DHCP option signature (match criteria)

dhcp-match-message-type

client-identity-mode commands

Configures the DHCP message type to match

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
dhcp-match-message-type [all|any|discover|request]
```

Parameters

```
dhcp-match-message-type [all|any|discover|request]
```

dhcp-match-message-type [all|any|discover|request]	Specifies the DHCP message type to consider for matching • all – Matches all message types: discover and request. Indicates that the fingerprint is checked with both the DHCP request and the DHCP discover message. • any – Matches any message type: discover or request. Indicates that the fingerprint is checked with either the DHCP request or the DHCP discover message. • discover – Matches discover messages only. Client matches the client identity only if the discover message sent by the client matches. Values configured for request messages are ignored • request – Matches request messages only. Client matches the client identity only if the request message sent by the client matches. Values configured for discover messages are ignored

Example

```
rfs4000-229D58(config-client-identity-test)#dhcp-match-message-type all
rfs4000-229D58(config-client-identity-test)#

rfs4000-229D58(config-client-identity-test)#show context
client-identity test
 dhcp 2 message-type discover option 2 exact hexstring 012456c22c44
 dhcp 1 message-type request option 60 exact ascii MSFT5.0
 dhcp-match-message-type all
rfs4000-229D58(config-client-identity-test)#
```

Related Commands:

no	Removes the DHCP message type to match

no

client-identity-mode commands

Removes the DHCP options match criteria configurations

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no [dhcp|dhcp-match-message-type]
```

Parameters

```
no [dhcp <1-16>|dhcp-match-message-type]
```

dhcp <1-16>	Removes the DHCP option match criteria rule identified by the <1-16> keyword • <1-16> – Specify the DHCP option match criteria rule index
dhcp-match-message-type	Removes the DHCP message type to match

Example

```
The following example shows the client identity 'test' settings before the
'no' commands are executed:

rfs4000-229D58(config-client-identity-test)#show context
client-identity test
 dhcp 2 message-type discover option 2 exact hexstring 012456c22c44
 dhcp 1 message-type request option 60 exact ascii MSFT5.0
 dhcp-match-message-type all
rfs4000-229D58(config-client-identity-test)#

The following example shows the client identity 'test' settings after the 'no'
commands are executed:

rfs4000-229D58(config-client-identity-test)#no dhcp 2

rfs4000-229D58(config-client-identity-test)#no dhcp-match-message-type

rfs4000-229D58(config-client-identity-test)#show context
client-identity test
 dhcp 1 message-type request option 60 exact ascii MSFT5.0
rfs4000-229D58(config-client-identity-test)#
```

Related Commands:

dhcp	Configures the DHCP option match criteria for device fingerprinting
dhcp-match-message-type	Configures the DHCP message type for device fingerprinting

client-identity-group

client-identity

The following table summarizes the commands for creating and configuring a new client identity group.

Command	Description	Reference
client-identity-group	Creates a new client identity group and enters its configuration mode	page 209
client-identity-group-mode commands	Invokes the client identity group configuration mode commands	page 211
client-identity	Creates new client identity policy and enters its configuration mode	page 203

client-identity-group

client-identity-group

Configures a new client identity group

A client identity group is a collection of client identities. Each client identity included in a client identity group is set a priority value that indicates the priority for that identity when device fingerprinting.

Device Fingerprinting relies on specific information sent by a wireless client when acquiring IP address and other configuration information from a DHCP server. The feature uses the DHCP options sent by the wireless client in the DHCP request or discover packets to derive a unique signature specific to the class of devices. For example, Apple devices have a different signature than Android devices. This unique signature can then be used to classify the devices and assign permissions and restrictions on each device class.

A client identity group can be attached to a profile or device, enabling device fingerprinting on them.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
client-identity-group <CLIENT-IDENTITY-GROUP-NAME> precedence <1-10000>
```

Parameters

```
client-identity-group <CLIENT-IDENTITY-GROUP-NAME> <1-10000>
```

client-identity-group <CLIENT-IDENTITY-GROUP-NAME>	Creates a new client identity group and enters its configuration mode • <CLIENT-IDENTITY-GROUP-NAME> – Specify a client identity group name. If the group does not exist, it is created.
precedence <1-10000>	Specifies a precedence value for this client identity match criteria in this client identity group Client identity signatures with lower precedence are evaluated first.

Example

```
rfs4000-229D58(config)#client-identity-group test
rfs4000-229D58(config-client-identity-group-test)#

rfs4000-229D58(config-client-identity-group-test)#?
Client Identity group Mode commands:
  client-identity  Client identity (DHCP Device Fingerprinting)
  no               Negate a command or set its defaults

  clrscr           Clears the display screen
  commit           Commit all changes made in this session
  do               Run commands from Exec mode
  end              End current mode and change to EXEC mode
  exit             End current mode and down to previous mode
  help             Description of the interactive help system
  revert           Revert changes
  service          Service Commands
  show             Show running system information
  write            Write running configuration to memory or terminal
```

```
rfs4000-229D58(config-client-identity-group-test)#
```

client-identity-group-mode commands

client-identity-group

The following table summarizes a new client identity group configuration mode commands.

Command	Description	Reference
client-identity	Associates an existing and configured client identity (device fingerprinting) with this client identity group	page 211
no	Removes the client identity associated with this client identity group	page 208

client-identity

client-identity-group-mode commands

Associates an existing and configured client identity (device fingerprinting) with this client identity group

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
client-identity <CLIENT-IDENTITY-NAME> precedence <1-10000>
```

Parameters

```
client-identity <CLIENT-IDENTITY-NAME> precedence <1-10000>
```

client-identity <CLIENT-IDENTITY-NAME>	Associates a client identity with this group • <CLIENT-IDENTITY-NAME> – Specify a client identity name (should be existing and configured)
precedence <1-10000>	Determines the order in which client identity is used. <1-10000> – Specify this client identity precedence from <1-10000>. The client identity rule is applied based on its precedence value. Lower the value, higher is the precedence. Therefore, a client identity with precedence 5 will get precedence over a client identity having precedence 20.

Example

```
The following example shows two client identities created and configured:

rfs4000-229D58(config)#show context
!
! Configuration of Brocade Mobility RFS4000 version 5.5.0.0-018D
!
!
version 2.1
!
!
```

```
client-identity TestClientIdentity
 dhcp 1 message-type request option-codes exact hexstring 5e4d36780b3a7f
!
client-identity test
 dhcp 2 message-type discover option 2 exact hexstring 012456c22c44
 dhcp 1 message-type request option 60 exact ascii MSFT5.0
 dhcp-match-message-type all
!
client-identity-group ClientIdentityGroup
 client-identity TestClientIdentity precedence 1
!
client-identity-group test
!
ip access-list BROADCAST-MULTICAST-CONTROL
 permit tcp any any rule-precedence 10 rule-description "permit all TCP
traffic"
 permit udp any eq 67 any eq dhcpc rule-precedence 11 rule-description "permit
D
--More--
rfs4000-229D58(config)#
```

The following example associates client identity ‘test’ with the client identity group ‘test’:

```
rfs4000-229D58(config-client-identity-group-test)#client-identity test
precedence 1
```

The following example shows the client identity group ‘test’ with two associated client identities having precedence 1 and 2:

```
rfs4000-229D58(config-client-identity-group-test)#client-identity
TestClientIdentity precedence 2
rfs4000-229D58(config-client-identity-group-test)#show context
client-identity-group test
 client-identity test precedence 1
 client-identity TestClientIdentity precedence 2
rfs4000-229D58(config-client-identity-group-test)#
```

The following example shows the possible client identities:

```
rfs4000-229D58(config)#show context
!
! Configuration of Brocade Mobility RFS4000 version 5.5.0.0-071B
!
!
version 2.3
!
!
client-identity Android-2-2
 dhcp 1 message-type request option 55 exact hexstring 01792103061c333a3b
 dhcp 6 message-type request option 60 exact ascii "dhcpcd 4.0.15"
!
client-identity Android-2-3
 dhcp 3 message-type request option 55 exact hexstring 01792103061c333a3b
 dhcp 6 message-type request option 60 exact ascii "dhcpcd 4.0.15"
 dhcp 1 message-type request option-codes exact hexstring 353d32393c37
 dhcp 2 message-type request option-codes exact hexstring 353d3236393c37
 dhcp 10 message-type request option-codes exact hexstring 353d3236393c0c37
!
client-identity Android-2-3-x
```

```
 dhcp 10 message-type request option 55 exact hexstring 01792103060f1c333a3b77
 dhcp 11 message-type request option 55 exact hexstring
01792103060f1c2c333a3b77
 dhcp 12 message-type request option 60 exact ascii "dhcpcd 4.0.15"
!
client-identity Android-3
 dhcp 4 message-type request option 55 exact hexstring 012103061c333a3b
 dhcp 5 message-type request option 60 starts-with ascii dhcpcd-5.2.10
 dhcp 6 message-type request option-codes exact hexstring 3532393c0c37
 dhcp 7 message-type request option-codes exact hexstring 35393c0c37
 dhcp 8 message-type request option-codes exact hexstring 353236393c0c37
!
client-identity Android-4
 dhcp 8 message-type request option 55 exact hexstring 012103061c333a3b
 dhcp 9 message-type request option 60 starts-with ascii dhcpcd-5.2.10
 dhcp 10 message-type request option 60 starts-with ascii
dhcpcd-5.2.10:Linux-3
!
client-identity Android-4-1-X
 dhcp 1 message-type request option 55 exact hexstring 012103060f1c333a3b
 dhcp 2 message-type request option 60 exact ascii dhcpcd-5.2.10
!
client-identity Android-4-2-X
 dhcp 1 message-type request option 55 exact hexstring 012103060f1c333a3b
 dhcp 2 message-type request option 60 exact ascii dhcpcd-5.5.6
!
client-identity Galaxy-Note
 dhcp 8 message-type request option 55 exact hexstring 012103061c333a3b
 dhcp 9 message-type request option 60 exact ascii
dhcpcd-5.2.10:Linux-3.0.15-N7000DDLP8-CL551076:armv7l:SMDK4210
!
client-identity Galaxy-Tab
 dhcp 8 message-type request option 55 exact hexstring 012103061c333a3b
 dhcp 9 message-type request option 60 exact ascii
dhcpcd-5.2.10:Linux-2.6.36.3:armv7l:p3
 dhcp 10 message-type request option-codes exact hexstring 353d3236393c0c37
 dhcp 11 message-type request option-codes exact hexstring 353d32393c0c37
!
client-identity Mac-OS-X
 dhcp 3 message-type request option 55 exact hexstring 0103060f775ffc2c2e2f
!
client-identity brocade-XOOM
 dhcp 9 message-type request option 55 exact hexstring 012103061c333a3b
 dhcp 10 message-type request option 60 exact ascii
dhcpcd-5.2.10:Linux-2.6.36.3-00042-g3c1a41e:armv7l:stingray
 dhcp 11 message-type request option-codes exact hexstring 3532393c0c37
 dhcp 12 message-type request option-codes exact hexstring 35393c0c37
 dhcp 13 message-type request option-codes exact hexstring 353236393c0c37
!
client-identity Ubuntu-11
 dhcp 2 message-type request option 55 exact hexstring
011c02030f06770c2c2f1a792a79f9fc2a
 dhcp 1 message-type request option-codes exact hexstring 3536320c37
 dhcp 3 message-type request option-codes exact hexstring 350c37
 dhcp 5 message-type request option-codes exact hexstring 35320c37
!
client-identity Windows-7
 dhcp 2 message-type request option 55 exact hexstring
010f03062c2e2f1f2179f92b
 dhcp 9 message-type request option 60 exact ascii "MSFT 5.0"
```

```
!
client-identity Windows-8
 dhcp 1 message-type request option 55 exact hexstring
010f03062c2e2f1f2179f9fc2b
 dhcp 5 message-type request option 60 exact ascii "MSFT 5.0"
!
client-identity Windows-Phone-7-5
 dhcp 11 message-type request option 55 exact hexstring 0103060f2c2e2f
 dhcp 12 message-type request option-codes exact hexstring 3536323d37
!
client-identity Windows-XP
 dhcp 4 message-type request option 55 exact hexstring 010f03062c2e2f1f21f92b
 dhcp 5 message-type request option 60 exact ascii "MSFT 5.0"
!
client-identity iPhone-iPad
 dhcp 10 message-type request option 55 exact hexstring 0103060f77fc
 dhcp 1 message-type request option-codes exact hexstring 3537393d32330c
 dhcp 2 message-type request option-codes exact hexstring 3537393d32360c
 dhcp 3 message-type request option-codes exact hexstring 3537393d3233
!
client-identity-group default
 client-identity Windows-XP precedence 100
 client-identity Windows-7 precedence 200
 client-identity Android-2-3 precedence 300
 client-identity Android-2-2 precedence 400
 client-identity Android-2-3-x precedence 500
 client-identity Galaxy-Tab precedence 600
 client-identity Brocade-XOOM precedence 700
 client-identity Android-3 precedence 800
 client-identity Galaxy-Note precedence 900
 client-identity Android-4 precedence 1000
 client-identity iPhone-iPad precedence 1100
 client-identity Ubuntu-11 precedence 1200
 client-identity Windows-Phone-7-5 precedence 1300
 client-identity Windows-8 precedence 1500
 client-identity Mac-OS-X precedence 1600
 client-identity Android-4-1-X precedence 1700
 client-identity Android-4-2-X precedence 1800
!
--More--
```

Related Commands:

no	Removes the client identity associated with the client identity group

no

client-identity-group-mode commands

Removes the client identity associated with the client identity group

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no client-identity <CLIENT-IDENTITY-NAME>
```

Parameters

```
no client-identity <CLIENT-IDENTITY-NAME>
```

no client-identity <CLIENT-IDENTITY-NAME>	Disassociates a specified client identity from this client identity group • <CLIENT-IDENTITY-NAME> – Specify the client identity name.

Example

```
rfs4000-229D58(config-client-identity-group-test)#show context
client-identity-group test
 client-identity test precedence 1
rfs4000-229D58(config-client-identity-group-test)#

rfs4000-229D58(config-client-identity-group-test)#no client-identity test
rfs4000-229D58(config)#
```

Related Commands:

client-identity	Associates an existing and configured client identity (device fingerprinting) with this client identity group

clone

Global Configuration Commands

Creates a replica of an existing object or device. The configuration of the new object or device is an exact copy of the existing object or device configuration. Use this command to copy existing configurations and then modifying only the required parameters.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
clone [TLO|device]

clone TLO <EXISTING-OBJECT-NAME> <NEW-OBJECT-NAME>

clone device <EXISTING-DEVICE-MAC/NAME> <NEW-DEVICE-MAC>
```

Parameters

	`clone TLO <EXISTING-OBJECT-NAME> <NEW-OBJECT-NAME>`
TLO <EXISTING-OBJECT-NAME> <NEW-OBJECT-NAME>	Creates a new TLO by cloning an existing top-level object. The new object has the same configuration as the cloned object. • <EXISTING-OBJECT-NAME> – Specify the existing object's (to be cloned) name • <NEW-OBJECT-NAME> – Provide the new object's name. **NOTE:** Enter clone and press **Tab** to list objects available for cloning.

	`clone device <EXISTING-DEVICE-MAC/NAME> <NEW-DEVICE-MAC/NAME>`
device <EXISTING-DEVICE-MAC/NAME> <NEW-DEVICE-MAC>	Configures a new device based on an existing device configuration • <EXISTING-DEVICE-MAC/NAME> – Specify the existing device's name or MAC address (the device to be cloned) • <NEW-DEVICE-MAC> – Provide the new device's MAC address. **NOTE:** Enter clone > device and press **Tab** to list devices available for cloning.

Example

```
rfs7000-37FABE(config)#clone rf_domain RF_Domain_Cloned RF_Domain_New
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show context
!
! Configuration of Brocade Mobility RFS7000 version 5.5.0.0-018D
!
!
version 2.1
customize show-wireless-client mac ip vendor vlan radio-id state wlan location
radio-alias radio-type
.....................................................................
........
!
rf-domain RF_Domain_New
 location
 contact
 timezone
 country-code
--More--
rfs7000-37FABE(config)#
```

customize

Global Configuration Commands

Customizes the output of the summary CLI commands. Use this command to define the data displayed as a result of various show commands.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
customize
[hostname-column-width|show-wireless-client|show-wireless-client-stats|
          show-wireless-client-stats-rf|show-wireless-meshpoint|

show-wireless-meshpoint-neighbor-stats|show-wireless-meshpoint-neighbor-stats
-rf|

show-wireless-radio|show-wireless-radio-stats|show-wireless-radio-stats-rf]

customize hostname-column-width <1-64>

customize show-wireless-client (br-name <1-64>,auth,client-identity
<1-32>,bss,enc,
          hostname <1-64>,ip,last-active,location <1-64>,mac,radio-alias
<3-67>,radio-id,
          radio-type,role <1-32>,state,username <1-64>,vendor,vlan,wlan)

customize show-wireless-client-stats (hostname <1-64>,mac,rx-bytes,rx-errors,

rx-packets,rx-throughput,tx-bytes,tx-dropped,tx-packets,tx-throughput)

customize show-wireless-client-stats-rf (average-retry-number,error-rate,
          hostname
<1-64>,mac,noise,q-index,rx-rate,signal,snr,t-index,tx-rate)

customize show-wireless-meshpoint (br-mac,cfg-as-root,hops,hostname <1-64>,
          interface-ids,is-root,mesh-name <1-64>,mpid,next-hop-hostname
<1-64>,next-hop-ifid,
          next-hop-use-time,path-metric,root-bound-time,root-hostname
<1-64>,root-mpid)

customize show-wireless-meshpoint-neighbor-stats (br-hostname <1-64>,
          neighbor-hostname
<1-64>,neighbor-ifid,rx-bytes,rx-errors,rx-packets,
          rx-throughtput,tx-bytes,tx-dropped,tx-packets,tx-throughput)

customize show-wireless-meshpoint-neighbor-stats-rf (br-hostname <1-64>,
          average-retry-number,error-rate,neighbor-hostname
<1-64>,neighbor-ifid,noise,
          q-index,rx-rate,signal,snr,t-index,tx-rate)

customize show-wireless-radio (adopt-to,br-name <1-64>,channel,location
<1-64>,
          num-clients,power,radio-alias
<3-67>,radio-id,radio-mac,rf-mode,state)

customize show-wireless-radio-stats (radio-alias
<3-67>,radio-id,radio-mac,rx-bytes,

rx-errors,rx-packets,rx-throughput,tx-bytes,tx-dropped,tx-packets,tx-throughp
ut)

customize show-wireless-radio-stats-rf
(average-retry-number,error-rate,noise,
          q-index,radio-alias
<3-67>,radio-id,radio-mac,rx-rate,signal,snr,t-index,tx-rate)
```

Parameters

	`customize hostname-column-width <1-64>`
hostname-column-width <1-64>	Configures default width of the hostname column in all show commands • <1-64> – Sets the hostname column width from 1 - 64 characters

	`customize show-wireless-client (br-name <1-64>,auth,client-identity <1-32>, bss,enc,hostname <1-64>,ip,last-active,location <1-64>,mac,radio-alias <3-67>, radio-id,radio-type,role <1-32>,state,username <1-64>,vendor,vlan,wlan)`
show-wireless-client	Customizes the show wireless client command output
br-name <1-64>	Includes the br-name column, which displays the name of the AP with which this client associates • <1-64> – Sets the br-name column width from 1 - 64 characters
auth	Includes the auth column, which displays the authorization protocol used by the wireless client
client-identity <1-32>	Includes the client-identity (device type) column, which displays details gathered from DHCP device fingerprinting feature (when enabled). For more information, see *client-identity*. • <1-32> – Sets the client-identity column width from 1 - 32 characters
bss	Includes the BSS column, which displays the BSS ID the wireless client is associated with
enc	Includes the enc column, which displays the encryption suite used by the wireless client
hostname <1-64>	Includes the hostname column, which displays the wireless client's hostname • <1-64> – Sets the hostname column width from 1 - 64 characters
ip	Includes the IP column, which displays the wireless client's current IP address
last-active	Includes the last-active column, which displays the time of last activity seen from the wireless client
location <1-64>	Includes the location column, which displays the location of the client's associated access points • <1-64> – Sets the location column width from 1 - 64 characters
mac	Includes the MAC column, which displays the wireless client's MAC address
radio-alias <3-67>	Includes the radio-alias column, which displays the radio alias with the AP's hostname and radio interface number in the "HOSTNAME:RX" format • <3-64> – Sets the radio-alias column width from 3 - 67 characters
radio-id	Includes the radio-id column, which displays the radio ID with the AP's MAC address and radio interface number in the "AA-BB-CC-DD-EE-FF:RX" format
radio-type	Includes the radio-type column, which displays the wireless client's radio type
role <1-32>	Includes the role column, which displays the client's role • <1-32> – Sets the role column width from 1 - 32 characters
state	Includes the state column, which displays the wireless client's current availability state
username <1-64>	Includes the username column, which displays the wireless client's username • <1-64> – Specify the username column width from 1 - 64 characters.
vendor	Includes the vendor column, which displays the wireless client's vendor ID
vlan	Includes the VLAN column, which displays the wireless client's assigned VLAN
wlan	Includes the WLAN column, which displays the wireless client's assigned WLAN

	`customize show-wireless-client-stats (hostname <1-64>,mac,rx-bytes,rx-errors, rx-packets,rx-throughput,tx-bytes,tx-dropped,tx-packets,tx-throughput)`
show-wireless-client-stats	Customizes the show wireless client stats command output
hostname <1-64>	Includes the hostname column, which displays the wireless client's hostname • <1-64> – Sets the hostname column width from 1 - 64 characters
mac	Includes the MAC column, which displays the wireless client's MAC address

rx-bytes	Includes the rx-bytes column, which displays the total number of bytes received by the wireless client
rx-errors	Includes the rx-error column, which displays the total number of errors received by the wireless client
rx-packets	Includes the rx-packets column, which displays the total number of packets received by the wireless client
rx-throughput	Includes the rx-throughput column, which displays the receive throughput at the wireless client
tx-bytes	Includes the tx-bytes column, which displays the total number of bytes transmitted by the wireless client
tx-dropped	Includes the tx-dropped column, which displays the total number of dropped packets by the wireless client
tx-packets	Includes the tx-packets column, which displays the total number of packets transmitted by the wireless client
tx-throughput	Includes the tx-throughput column, which displays the transmission throughput at the wireless client
	`customize show-wireless-client-stats-rf (average-retry-number,error-rate,noise, q-index,rx-rate,signal,snr,t-index,tx-rate)`
show-wireless-client-stats-rf	Customizes the show wireless client stats RF command output
average-retry-number	Includes the average-retry-number column, which displays the average number of retransmissions made per packet
error-rate	Includes the error-rate column, which displays the rate of error for the wireless client
hostname <1-64>	Includes the hostname column, which displays the wireless client's hostname • <1-64> – Sets the hostname column width from 1 - 64 characters
mac	Includes the MAC column, which displays the wireless client's MAC address
noise	Includes the noise column, which displays the noise (in dBm) as detected by the wireless client
q-index	Includes the q-index column, which displays the RF quality index **NOTE:** Higher values indicate better RF quality.
rx-rate	Includes the rx-rate column, which displays the receive rate at the particular wireless client
signal	Includes the signal column, which displays the signal strength (in dBm) at the particular wireless client
snr	Includes the snr column, which displays the *signal to noise* (SNR) ratio (in dB) at the particular wireless client
t-index	Includes the t-index column, which displays the traffic utilization index at the particular wireless client
tx-rate	Includes the tx-rate column, which displays the packet transmission rate at the particular wireless client
	`customize show-wireless-meshpoint (br-mac,cfg-as-root,hops,hostname <1-64>, interface-ids,is-root,mesh-name <1-64>,mpid,next-hop-hostname <1-64>,next-hop-ifid, next-hop-use-time,path-metric,root-bound-time,root-hostname <1-64>,root-mpid)`
show-wireless-meshpoint	Customizes the show wireless meshpoint command output
br-mac	Includes the br-name column, which displays the AP's MAC address in the AA-BB-CC-DD-EE-FF format. Applicable only in case of non-controller meshpoints
cfg-as-root	Includes the cfg-as-root column, which displays the configured root state of the meshpoint
hops	Includes the hops column, which displays the number of hops to the root for this meshpoint
hostname <1-64>	Includes the hostname column, which displays the AP's hostname. Applicable only in case of non-wireless controller meshpoints • <1-64> – Sets the hostname column width from 1 - 64 characters
interface-ids	Includes the interface-ids column, which displays the interface identifiers (interfaces used by this meshpoint)

is-root	Includes the is-root column, which displays the current root state of the meshpoint
mesh-name <1-64>	Includes the mesh-name column, which displays the meshpoint's name • <1-64> – Sets the mesh-name column width from 1 - 64 characters
mpid	Includes the mpid column, which displays the meshpoint identifier in the AA-BB-CC-DD-EE-FF format
next-hop-hostname <1-64>	Includes the next-hop-hostname column, which displays the next-hop AP's name (the AP next in the path to the bound root) • <1-64> – Sets the next-hop-hostname column width from 1 - 64 characters
next-hop-ifid	Includes the next-hop-ifid column, which displays the next-hop interface identifier in the AA-BB-CC-DD-EE-FF format
next-hop-use-time	Includes the next-hop-use-time column, which displays the time since this meshpoint started using this next hop
root-bound-time	Includes the root-bound-time column, which displays the time since this meshpoint has been bound to the current root
root-hostname <1-64>	Includes the root-hostname column, which displays the root AP's hostname to which this meshpoint is bound • <1-64> – Sets the root-hostname column width from 1 - 64 characters
root-mpid	Includes the root-mpid column, which displays the bound root meshpoint identifier in the AA-BB-CC-DD-EE-FF format
	`customize show-wireless-meshpoint-neighbor-stats (br-hostname <1-64>, neighbor-hostname <1-64>,neighbor-ifid,rx-bytes,rx-errors,rx-packets,rx-throughtput, tx-bytes,tx-dropped,tx-packets,tx-throughput)`
show-wireless-meshpoint-neighbor-stats	Customizes the show wireless meshpoint neighbor stats command output
br-name <1-64>	Includes the br-name column, which displays name of the AP reporting a neighbor • <1-64> – Sets the br-name column width from 1 - 64 characters
neighbor-hostname <1-64>	Includes the neighbor-hostname column, which displays the reported neighbor's hostname • <1-64> – Sets the neighbor-hostname column width from 1 - 64 characters
neighbor-ifid	Includes the neighbor-ifid column, which displays the neighbor's interface ID
rx-bytes	Includes the rx-bytes column, which displays the total bytes received
rx-errors	Includes the rx-error column, which displays the total bytes of error received
rx-packets	Includes the rx-packets column, which displays the number of packets received
rx-throughput	Includes the rx-throughput column, which displays neighbor's received throughput
tx-bytes	Includes the tx-bytes column, which displays the total bytes transmitted
tx-dropped	Includes the tx-dropped column, which displays the total bytes dropped
tx-packets	Includes the tx-packets column, which displays the number of packets transmitted
tx-throughput	Includes the tx-throughput column, which displays neighbor's transmitted throughput
	`customize show-wireless-meshpoint-neighbor-stats-rf (br-hostname <1-64>, average-retry-number,error-rate,neighbor-hostname <1-64>,neighbor-ifid,noise,q-index, rx-rate,signal,snr,t-index,tx-rate)`
show-wireless-meshpoint-neighbor-stats-rf	Customizes the show wireless meshpoint neighbor statistics RF command output
br-name <1-64>	Includes the br-name column, which displays name of the AP reporting a neighbor • <1-64> – Sets the br-name column width from 1 - 64 characters

average-retry-number	Includes the average-retry-number column, which displays the average number of retransmissions made per packet.
error-rate	Includes the error-rate column
neighbor-hostname <1-64>	Includes the neighbor-hostname, which displays reported neighbor's hostname • <1-64> – Sets the neighbor-hostname column width from 1 - 64 characters
noise	Includes the noise column, which displays the noise level in dBm
q-index	Includes the q-index column, which displays the q-index
rx-rate	Includes the rx-rate column, which displays rate of receiving
signal	Includes the signal column, which displays the signal strength in dBM
snr	Includes the snr column, which displays the signal-to-noise ratio
t-index	Includes the t-index column, which displays t-index
tx-rate	Includes the tx-rate column, which displays rate of transmission
	`customize show-wireless-radio (adopt-to,br-name <1-64>,channel,location <1-64>, num-clients,power,radio-alias <3-67>,radio-id,radio-mac,rf-mode,state)`
show-wireless-radio	Customizes the show wireless radio command output
adopt-to	Includes the adopt-to column, which displays information about the wireless controller adopting this AP
br-name <1-64>	Includes the br-name column, which displays information about the AP this radio belongs • <1-64> – Sets the br-name column width from 1 - 64 characters
channel	Includes the channel column, which displays information about the configured and current channel for this radio
location <1-64>	Includes the location column, which displays the location of the AP this radio belongs • <1-64> – Sets the location column width from 1 - 64 characters
num-clients	Includes the num-clients column, which displays the number of clients associated with this radio
power	Includes the power column, which displays the radio's configured and current transmit power
radio-alias <3-67>	Includes the radio-alias column, which displays the radio's alias (combination of AP's hostname and radio interface number in the "HOSTNAME:RX" formate) • <3-67> – Sets the radio-alias column width from 3 - 67 characters
radio-id	Includes the radio-id column, which displays the radio's ID (combination of AP's MAC address and radio interface number in the "AA-BB-CC-DD-EE-FF:RX" format)
radio-mac	Includes the radio-mac column, which displays the radio's base MAC address
rf-mode	Includes the rf-mode column, which displays the radio's operating mode. The radio mode can be 2.4 GHz, 5.0 GHz, or sensor.
state	Includes the state column, which displays the radio's current operational state
	`customize show-wireless-radio-stats (radio-alias <3-67>,radio-id,radio-mac, rx-bytes,rx-errors,rx-packets,rx-throughput,tx-bytes,tx-dropped,tx-packets, tx-throughput)`
show-wireless-radio-stats	Customizes the show wireless radio statistics command output
radio-alias <3-67>	Includes the radio-alias column, which displays the radio's alias (combination of AP's hostname and radio interface number in the "HOSTNAME:RX" format) • <3-67> – Sets the radio-alias column width from 3 - 67 characters
radio-id	Includes the radio-id column, which displays the radio's ID (combination of AP's MAC address and radio interface number in the "AA-BB-CC-DD-EE-FF:RX" format)

radio-mac	Includes the radio-mac column, which displays the radio's base MAC address
rx-bytes	Includes the rx-bytes column, which displays the total number of bytes received by the radio
rx-errors	Includes the rx-error column, which displays the total number of errors received by the radio
rx-packets	Includes the rx-packets column, which displays the total number of packets received by the radio
rx-throughput	Includes the rx-throughput column, which displays the receive throughput at the radio
tx-bytes	Includes the tx-bytes column, which displays the total number of bytes transmitted by the radio
tx-dropped	Includes the tx-dropped column, which displays the total number of packets dropped by the radio
tx-packets	Includes the tx-packets column, which displays the total number of packets transmitted by the radio
tx-throughput	Includes the tx-throughput column, which displays the transmission throughput at the radio

```
customize show-wireless-radio-stats-rf
(average-retry-number,error-rate,noise,
q-index,radio-alias
<3-67>,radio-id,radio-mac,rx-rate,signal,snr,t-index,tx-rate)
```

show-wireless-radio-stats-rf	Customizes the show wireless radio stats RF command output
average-retry-number	Includes the average-retry-number column, which displays the average number of retransmissions per packet
error-rate	Includes the error-rate column, which displays the rate of error for the radio
noise	Includes the noise column, which displays the noise detected by the radio
q-index	Includes the q-index column, which displays the RF quality index **NOTE:** Higher values indicate better RF quality.
radio-alias <3-67>	Includes the radio-alias column, which displays the radio's alias (combination of AP's hostname and radio interface number in the "HOSTNAME:RX" format) • <3-67> – Sets the radio-alias column width from 3 - 67 characters
radio-id	Includes the radio-id column, which displays the radio's ID (combination of AP's MAC address and radio interface number in the "AA-BB-CC-DD-EE-FF:RX" format)
radio-mac	Includes the radio-mac column, which displays the radio's base MAC address
rx-rate	Includes the rx-rate column, which displays the receive rate at the particular radio
signal	Includes the signal column, which displays the signal strength at the particular radio
snr	Includes the snr column, which displays the signal-to-noise ratio at the particular radio
t-index	Includes the t-index column, which displays the traffic utilization index at the particular radio
tx-rate	Includes the tx-rate column, which displays the packet transmission rate at the particular radio

Example

```
rfs7000-37FABE(config)#customize show-wireless-client br-name auth

rfs7000-37FABE(config)#commit

rfs7000-37FABE(config)#show wireless client
-----------------------
          AP-NAME  AUTH
-----------------------
-----------------------
Total number of wireless clients displayed: 0
rfs7000-37FABE(config)#
```

The following examples demonstrate how to customize the *show* > *wireless* > *meshpoint* command output.

The following example shows the *show* > *wireless* > *meshpoint* command output format before customization:

```
rfs4000-1B3596#show wireless meshpoint
-------------------------------------------------------------------------------
-------------------------------------------------------------
MESH           HOSTNAME        HOPS IS-ROOT CONFIG-AS-ROOT ROOT-HOSTNAME
ROOT-BOUND-TIME NEXT-HOP-HOSTNAME NEXT-HOP-USE-TIME
-------------------------------------------------------------------------------
-------------------------------------------------------------
c00466          br7131-96F998       1 NO     NO           br7131-96FAAC
1 days 02:01:33 br7131-96FAAC       1 days 02:01:33
c00466         br7131-96FAAC      0 YES    YES         N/A
N/A N/A                            N/A
c00466          br7131-96F6B4       2 NO     NO           br7131-96FAAC
1 days 02:01:31 br7131-96F998       1 days 02:01:31
Total number of meshpoint displayed: 3
rfs4000-1B3596#
```

The *show* > *wireless* > *meshpoint* command output is customized as follows:

```
rfs4000-1B3596(config)#customize show-wireless-meshpoint hops hostname 13
is-root cfg-as-root root-bound-time next-hop-hostname next-hop-use-time
interface-ids
rfs4000-1B3596(config)#commit
```

The following example shows the *show* > *wireless* > *meshpoint* command output format after customization:

```
rfs4000-1B3596(config)#show wireless meshpoint
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
--------------------
HOPS HOSTNAME      IS-ROOT CONFIG-AS-ROOT   ROOT-BOUND-TIME NEXT-HOP-HOSTNAME
NEXT-HOP-USE-TIME INTERFACE-IDENTIFIERS
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
--------------------
   1 br7131-96F998 NO     NO             1 days 02:10:04 br7131-96FAAC      1
days 02:10:04 00-23-68-93-16-60(00-23-68-96-F9-98:R1),
00-23-68-93-48-E1(00-23-68-96-F9-98:R2)
  0 br7131-96FAAC YES    YES                    N/A N/A
N/A 00-23-68-95-23-51(00-23-68-96-FA-AC:R2)
   2 br7131-96F6B4 NO     NO             1 days 02:10:08 br7131-96F998      1
days 02:10:08 00-23-68-95-33-31(00-23-68-96-F6-B4:R2)
Total number of meshpoint displayed: 3
rfs4000-1B3596(config)#
```

To revert to the default format use the *no* > *customize* command.

```
rfs4000-1B3596(config)#no customize show-wireless-meshpoint
rfs4000-1B3596(config)#commit
```

The *show* > *wireless* > *meshpoint* command output format has been reverted to default.

```
rfs4000-1B3596(config)#show wireless meshpoint
```

```
-------------------------------------------------------------------------------
-------------------------------------------------------
MESH            HOSTNAME        HOPS IS-ROOT CONFIG-AS-ROOT ROOT-HOSTNAME
ROOT-BOUND-TIME NEXT-HOP-HOSTNAME NEXT-HOP-USE-TIME
-------------------------------------------------------------------------------
-------------------------------------------------------
c00466           br7131-96F998       1 NO     NO           br7131-96FAAC
1 days 02:10:40 br7131-96FAAC       1 days 02:10:40
c00466         br7131-96FAAC      0 YES    YES         N/A
N/A N/A                             N/A
c00466           br7131-96F6B4       2 NO     NO           br7131-96FAAC
1 days 02:10:38 br7131-96F998       1 days 02:10:38
Total number of meshpoint displayed: 3
rfs4000-1B3596(config)#
```

Related Commands:

no	Restores custom CLI settings to default
wireless	Displays wireless configuration and other information

device

Global Configuration Commands

Enables simultaneous configuration of multiple devices

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
device {containing|filter}

device containing <STRING> {filter type [br650|br6511|br1220|
          |br71xx|br81xx|rfs4000|rfs6000|rfs7000]}

device filter type [br650|br6511|br1220|br71xx|
          br81xx|rfs4000|rfs6000|rfs7000]
```

Parameters

```
device containing <STRING> {filter type [br650|br6511|br1220|
br71xx|br81xx|rfs4000|rfs6000|rfs7000]}
```

device	Configures a basic device profile
containing <STRING>	Configures the string to search for in the device's hostname. Only those devices that have the specified string in their hostname can be configured. • <STRING> – Specify the string to search for in the device's hostname
filter type	Optional. Filters out a specific device type

br650	Optional. Filters out devices other than Brocade Mobility 650 Access Points
br6511	Optional. Filters out devices other than Brocade Mobility 6511 Access Points
br1220	Optional. Filters out devices other than Brocade Mobility 1220 Access Points
br71xx	Optional. Filters out devices other than Brocade Mobility 71XX Access Points
rfs4000	Optional. Filters out devices other than Brocade Mobility RFS4000s
rfs6000	Optional. Filters out devices other than Brocade Mobility RFS6000s
rfs7000	Optional. Filters out devices other than Brocade Mobility RFS7000s

```
device filter type [br650|br6511|br1220|br71xx|
br81xx|rfs4000|rfs6000|rfs7000]
```

device	Configures a basic device profile
filter-type	Filters out a specific device type
br650	Filters out devices other than Brocade Mobility 650 Access Points
br6511	Filters out devices other than Brocade Mobility 6511 Access Points
br1220	Filters out devices other than Brocade Mobility 1220 Access Points
br71xx	Filters out devices other than Brocade Mobility 71XX Access Points
rfs4000	Filters out devices other than Brocade Mobility RFS4000s
rfs6000	Filters out devices other than Brocade Mobility RFS6000s
rfs7000	Filters out devices other than Brocade Mobility RFS7000s

Example

```
rfs7000-37FABE(config)#device containing br filter type br71xx
% Error: Parsing cmd line (1)
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#device containing br filter type br650
rfs7000-37FABE(config-device-{'type': 'br650', 'con)#
```

Related Commands:

no	Removes multiple devices from the network

device-categorization

Global Configuration Commands

Categorizes devices as sanctioned or neighboring. Categorization of devices enables quick identification and blocking of unsanctioned devices in the network.

The following table lists the command to enter the device categorization configuration mode.

Command	Description	Reference
device-categorization	Creates a device categorization list and enters its configuration mode	page 226
device-categorization-mode commands	Summarizes device categorization list configuration mode commands	page 227

device-categorization

device-categorization

Configures a device categorization list

Proper classification and categorization of devices (access points, clients etc.) helps suppress unnecessary unauthorized access point alarms, allowing network administrators to focus on alarms on devices actually behaving in a suspicious manner. An intruder with a device erroneously authorized could potentially perform activities that harm your organization.

Authorized access points and clients are generally known to you and conform with your organization's security policies. Unauthorized devices are those detected as interoperating within the network, but are not approved. These devices should be filtered to avoid jeopardizing the data within a managed network. Use this command to apply the neighboring and sanctioned (approved) filters on peer devices operating within a wireless controller or access point's radio coverage area. Detected client MAC addresses can also be filtered based on their classification.

If a device categorization list does not exist, it is created.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
device-categorization <DEVICE-CATEGORIZATION-LIST-NAME>
```

Parameters

```
device-categorization <DEVICE-CATEGORIZATION-LIST-NAME>
```

<DEVICE-CATEGORIZATION-LIST-NAME>	Specify the device categorization list name. If a list with the same name does not exist, it is created.

Example

```
rfs7000-37FABE(config)#device-categorization rfs7000

rfs7000-37FABE(config-device-categorization-rfs7000)#?
Device Category Mode commands:
  mark-device  Add a device
  no           Negate a command or set its defaults

  clrscr       Clears the display screen
  commit       Commit all changes made in this session
  do           Run commands from Exec mode
  end          End current mode and change to EXEC mode
  exit         End current mode and down to previous mode
  help         Description of the interactive help system
  revert       Revert changes
  service      Service Commands
  show         Show running system information
  write        Write running configuration to memory or terminal
```

```
rfs7000-37FABE(config-device-categorization-rfs7000)#
```

Related Commands:

no	Removes an existing device categorization list

device-categorization-mode commands

device-categorization

The following table summarizes device categorization configuration commands.

Command	Description	Reference
mark-device	Adds a device to the device categorization list	page 227
no	Removes a device from the device categorization list	page 228
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

mark-device

device-categorization-mode commands

Adds a device to the device categorization list as sanctioned or neighboring. Devices are further classified as AP or client.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
mark-device <1-1000> [sanctioned|neighboring] [br|client]
mark-device <1-1000> [sanctioned|neighboring] br {mac <MAC>|ssid <SSID> {mac
<MAC>}}
mark-device <1-1000> [sanctioned|neighboring] client {mac <MAC>}
```

Parameters

	`mark-device <1-1000> [sanctioned|neighboring] br {mac <MAC>|ssid <SSID> {mac <MAC>}}`
<1-1000>	Configures the device categorization entry index number
sanctioned	Marks a device as sanctioned. A sanctioned device is authorized to use network resources.
neighboring	Marks a device as neighboring. A neighboring device is a neighbor in the same network as this device.
br {mac <MAC>| ssid <SSID>}	Marks a specified AP as sanctioned or neighboring based on its MAC address or SSID • mac <MAC> – Optional. Specify the AP's MAC address • ssid <SSID> – Optional. Specify the AP's SSID. After specifying the SSID, you can optionally specify its MAC SSID. **NOTE:** All APs are marked if no specific MAC address or SSID is provided.

	`mark-device [sanctioned|neighboring] client {mac <MAC>}`
<1-1000>	Configures the device categorization entry index number
sanctioned	Marks the wireless client as sanctioned. A sanctioned device is authorized to use network resources.
neighboring	Marks the wireless client as neighboring. A neighboring device is a neighbor in the same network as this device.
client {mac <MAC>}	Marks a specified wireless client as sanctioned or neighboring based on its MAC address • mac <MAC> – Optional. Specify the wireless client's MAC address

Example

```
rfs7000-37FABE(config-device-categorization-rfs7000)#mark-device 1 sanctioned
br
 mac 11-22-33-44-55-66

rfs7000-37FABE(config-device-categorization-rfs7000)#show context
device-categorization rfs7000
 mark-device 1 sanctioned br mac 11-22-33-44-55-66
rfs7000-37FABE(config-device-categorization-rfs7000)#
```

Related Commands:

no	Removes an entry from the device categorization list

no

device-categorization-mode commands

Removes a device from the device categorization list

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no mark-device <1-1000> [neighboring|sanctioned] [br|client]
no mark-device <1-1000> [sanctioned|neighboring] client {mac <MAC>}
```

```
no mark-device <1-1000> [sanctioned|neighboring] br {mac <MAC>|ssid <SSID>
{mac <MAC>}}
```

Parameters

```
no mark-device <1-1000> [sanctioned|neighboring] br {mac <MAC>|ssid <SSID>
{mac <MAC>}}
```

no mark-device	Removes a device from the marked devices list
<1-1000>	Specify the mark device entry index.
sanctioned	Removes a device marked as sanctioned
neighboring	Removes a device marked as neighboring
br {mac <MAC>| ssid <SSID>}	Removes a AP marked as sanctioned or neighboring based on its MAC address or SSID • mac <MAC> – Optional. Specify the AP's MAC address • ssid <SSID> – Optional. Specify the AP's SSID. After specifying the SSID, you can optionally specify its MAC SSID.

```
no mark-device <1-1000> [sanctioned|neighboring] client {mac <MAC>}
```

no mark-device	Removes a device from the marked devices list
<1-1000>	Specify the mark device entry index.
sanctioned	Removes a wireless client as sanctioned
neighboring	Removes a wireless client marked as neighboring
client {mac <MAC>}	Removes a wireless client marked as sanctioned or neighboring based on its MAC address • mac <MAC> – Optional. Specify the wireless client's MAC address.

Example

```
The following example shows the device categorization list 'rfs7000' settings
before the 'no' command is executed:

rfs7000-37FABE(config-device-categorization-rfs7000)#show context
device-categorization rfs7000
 mark-device 1 sanctioned br mac 11-22-33-44-55-66
rfs7000-37FABE(config-device-categorization-rfs7000)#

rfs7000-37FABE(config-device-categorization-rfs7000)#no mark-device 1
sanctioned br mac 11-22-33-44-55-66

The following example shows the device categorization list 'rfs7000' settings
after the 'no' command is executed:

rfs7000-37FABE(config-device-categorization-rfs7000)#show context
device-categorization rfs7000
rfs7000-37FABE(config-device-categorization-rfs7000)#
```

Related Commands:

mark-device	Adds a device to a list of sanctioned or neighboring devices

dhcp-server-policy

Global Configuration Commands

Configures DHCP server policy parameters, such as class, address range, and options. A new policy is created if it does not exist.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
dhcp-server-policy <DHCP-POLICY-NAME>
```

Parameters

```
dhcp-server-policy <DHCP-POLICY-NAME>
```

<DHCP-POLICY-NAME>	Specify the DHCP policy name. If the policy does not exist, it is created.

Example

```
rfs7000-37FABE(config)#dhcp-server-policy test
rfs7000-37FABE(config-dhcp-policy-test)#?
DHCP policy Mode commands:
  bootp       BOOTP specific configuration
  dhcp-class  Configure DHCP class (for address allocation using DHCP
              user-class options)
  dhcp-pool   Configure DHCP server address pool
  no          Negate a command or set its defaults
  option      Define DHCP server option
  ping        Specify ping parameters used by DHCP Server

  clrscr      Clears the display screen
  commit      Commit all changes made in this session
  do          Run commands from Exec mode
  end         End current mode and change to EXEC mode
  exit        End current mode and down to previous mode
  help        Description of the interactive help system
  revert      Revert changes
  service     Service Commands
  show        Show running system information
  write       Write running configuration to memory or terminal

rfs7000-37FABE(config-dhcp-policy-test)#
```

Related Commands:

no	Removes an existing DHCP server policy

NOTE
For more information on DHCP policy, see *Chapter 13, DHCP-SERVER-POLICY*.

dns-whitelist

Global Configuration Commands

Configures a DNS whitelist. A DNS whitelist is a list of domains allowed access to the network.

The following table lists DNS Whitelist configuration mode commands.

Command	Description	Reference
dns-whitelist	Creates a DNS whitelist and enters its configuration mode	page 231
dns-whitelist-mode commands	Summarizes DNS whitelist configuration mode commands	page 232

dns-whitelist

dns-whitelist

Configures a DNS whitelist. A DNS whitelist is a list of domains allowed access to the network.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
dns-whitelist <DNS-WHITELIST-NAME>
```

Parameters

```
dns-whitelist <DNS-WHITELIST-NAME>
```

<DNS-WHITELIST-NAME>	Specify the DNS whitelist name. If the whitelist does not exist, it is created.

Example

```
rfs7000-37FABE(config)#dns-whitelist test
rfs7000-37FABE(config-dns-whitelist-test)#?
DNS Whitelist Mode commands:
  no       Negate a command or set its defaults
  permit   Match a host

  clrscr   Clears the display screen
  commit   Commit all changes made in this session
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  revert   Revert changes
  service  Service Commands
  show     Show running system information
  write    Write running configuration to memory or terminal

rfs7000-37FABE(config-dns-whitelist-test)#
```

Related Commands:

no	Removes an existing DNS Whitelist

dns-whitelist-mode commands

dns-whitelist

The following table summarizes DNS Whitelist configuration mode commands.

Command	Description	Reference
permit	Permits a host, existing on a DNS whitelist, access to the network or captive portal	page 232
no	Negates a command or reverts to default	page 233
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

permit

dns-whitelist-mode commands

A whitelist is a list of host names and IP addresses permitted access to the network or captive portal. This command adds a device by its hostname or IP address to the DNS whitelist.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
permit <IP/HOSTNAME> {suffix}
```

Parameters

```
permit <IP/HOSTNAME> {suffix}
```

<IP/HOSTNAME>	Adds a device to the DNS whitelist • <IP/HOSTNAME> – Specify the devices' IP address or hostname. A maximum of 256 entries can be made.
suffix	Optional. Matches any hostname including the specified name as suffix

Example

```
rfs7000-37FABE(config-dns-whitelist-test)#permit motorolasolutions.com suffix

rfs7000-37FABE(config-dns-whitelist-test)#show context
dns-whitelist test
permit motorolasolutions.com suffix
rfs7000-37FABE(config-dns-whitelist-test)#
```

Related Commands:

no	Removes a DNS whitelist entry

no

dns-whitelist-mode commands

Removes a specified host or IP address from the DNS whitelist, and prevents it from accessing network resources

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no permit <IP/HOSTNAME>
```

Parameters

```
no permit <IP/HOSTNAME>
```

<IP/HOSTNAME>	Removes a device from the DNS whitelist (identifies the device by its IP address or hostname) • <IP/HOSTNAME> – Specify the device's IP address or hostname

Example

```
rfs7000-37FABE(config-dns-whitelist-test)#show context
dns-whitelist test
permit motorolasolutions.com suffix
rfs7000-37FABE(config-dns-whitelist-test)#

rfs7000-37FABE(config-dns-whitelist-test)#no permit motorolasolutions.com

rfs7000-37FABE(config-dns-whitelist-test)#show context
dns-whitelist test1
rfs7000-37FABE(config-dns-whitelist-test)#
```

Related Commands:

permit	Adds a device to the DNS whitelist

end

Global Configuration Commands

Ends and exits the current mode and moves to the PRIV EXEC mode

The prompt changes to the PRIV EXEC mode.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
end
```

Parameters

None

Example

```
rfs7000-37FABE(config)#end
rfs7000-37FABE#
```

event-system-policy

Global Configuration Commands

Configures how events are supported. Each event can be configured individually to perform an action such as sending an e-mail or forwarding a notification.

The following table lists event system configuration mode commands.

Command	Description	Reference
event-system-policy	Creates an event system policy and enters its configuration mode	page 234
event-system-policy-mode commands	Summarizes event system policy configuration mode commands	page 236

event-system-policy

event-system-policy

Configures a system wide events handling policy

Event system policies enable administrators to create notification mechanisms using one, some, or all of the SNMP, syslog, controller forwarding, or email notification options available to the controller or service platform. Each listed event can have customized notification settings defined and saved as part of an event policy. Thus, policies can be configured and administrated in respect to specific sets of client association, authentication or encryption, and performance events. Once policies are defined, they can be mapped to device profiles strategically as the likelihood of an event applies to particular devices.

To view an existing event system policy configuration details, use the *show* > *event-system-policy* command.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
event-system-policy <EVENT-SYSTEM-POLICY-NAME>
```

Parameters

```
event-system-policy <EVENT-SYSTEM-POLICY-NAME>
```

<EVENT-SYSTEM-POLICY-NAME>	Specify the event system policy name. If the policy does not exist, it is created.

Example

```
rfs7000-37FABE(config)#event-system-policy event-testpolicy

rfs7000-37FABE(config-event-system-policy-event-testpolicy)#?
Event System Policy Mode commands:
  event    Configure an event
  no       Negate a command or set its defaults

  clrscr   Clears the display screen
  commit   Commit all changes made in this session
  do       Run commands from Exec mode
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  revert   Revert changes
  service  Service Commands
  show     Show running system information
  write    Write running configuration to memory or terminal

rfs7000-37FABE(config-event-system-policy-event-testpolicy)#
```

Related Commands:

no	Removes an event system policy

event-system-policy-mode commands

event-system-policy

The following table summarizes event system policy configuration mode commands.

Command	Description	Reference
event	Configures an event	page 236
no	Negates a command or reverts to default	page 245
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

event

event-system-policy-mode commands

Configures an event and sets the action performed when the event happens

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
event <EVENT-TYPE> <EVENT-NAME> (email,forward-to-switch,snmp,syslog)
[default|on|off]
The even types are:

rfs7000-37FABE(config-event-system-policy-testpolicy)#event ?
  aaa             AAA/Radius module
  adv-wips        Adv-wips module
  br              Access Point module
  caching         Content Cache Service
  captive-portal  Captive Portal
  certmgr         Certificate Manager
  cfgd            Cfgd module
  cluster         Cluster module
  crm             Critical Resource Monitoring
  dhcpsvr         DHCP Configuration Daemon
```

```
  diag            Diag module
  dot11           802.11 management module
  dot1x           802.1X Authentication
  fwu             Firmware update module
  isdn            Isdn module
  l2tpv3          Layer 2 Tunneling Protocol Version 3
  licmgr          License module
  mesh            Mesh module
  mgmt            Management Services
  nsm             Network Services Module
  pm              Process-monitor module
  radconf         Radius Configuration Daemon
  radio           Radio module
  smrt            Smart-rf module
  smtpnot         Smtpnot module
  system          System module
  test            Test module
  vrrp            Virtual Router Redundancy Protocol
  test            Test module
  wips            Wireless IPS module

rfs7000-37FABE(config-event-system-policy-testpolicy)#
```

NOTE
The parameter values for <EVENT-TYPE> and <EVENT-NAME> are summarized in the table under the Parameters section.

Parameters

```
event <EVENT-TYPE> <EVENT-NAME> (email,forward-to-switch,snmp,syslog)
[default|on|off]
```

<event-type>	<event-name>
aaa	Configures authentication, authorization, and accounting related event messages • radius-discon-msg – RADIUS disconnection message • radius-session-expired – RADIUS session expired message • radius-session-not-started – RADIUS session not started message • radius-vlan-update – RADIUS VLAN update message
adv-wips	Configures advanced WIPS related event messages

<event-type>	<event-name>
br	Configures AP event messages • adopted – Event AP adopted message • adopted-to-controller – Event AP adopted to wireless controller message • br-adopted – Event access port adopted message • br-autoup-done – Event AP autoup done message • br-autoup-fail – Event AP autoup fail message • br-autoup-needed – Event AP autoup needed message • br-autoup-no-need – Event AP autoup not needed message • br-autoup-reboot – Event AP autoup reboot message • br-autoup-timeout – Event AP autoup timeout message • br-autoup-ver – Event AP autoup version message • br-reset-detected – Event access port reset detected message • br-reset-request – Event access port user requested reset message • br-timeout – Event access port timed out message • br-unadopted – Event access port unadopted message • image-parse-failure – Event image parse failure message • legacy-auto-update – Event legacy auto update message • no-image-file – Event no image file message • offline – Event AP detected as offline • online – Event offline AP detected as online • reset – Event reset message • sw-conn-lost – Event software connection lost message • unadopted – Event unadopted message
caching	Configures content cache service related event messages
captive-portal	Configures captive portal (hotspot) related event messages • allow-access – Event client allowed access message • auth-failed – Event authentication failed message • auth-success – Event authentication success message • client-disconnect – Event client disconnected message Contd..
	• client-removed – Event client removed message • data-limit-exceed – Event client data limit exceed message • flex-log-access – Event flexible log access granted to client message • inactivity-timeout – Event client time-out due to inactivity message • page-cre-failed – Event page creation failure message • purge-client – Event client purged message • session-timeout – Event session timeout message • vlan-switch – Event client switched VLAN

<event-type>	<event-name>
certmgr	Configures certificate manager related event messages • ca-cert-actions-failure – Event CA certificate actions failure message • ca-cert-actions-success – Event CA certificate actions success message • ca-key-actions-failure – Event CA key actions failure message • ca-key-actions-success – Event CA key actions success message • cert-expiry – Event certificate expiry message • crl-actions-failure – Event *Certificate Revocation List* (CRL) actions failure message • crl-actions-success – Event CRL actions success message • csr-export-failure – Event CSR export failure message • csr-export-success – Event CSR export success message • delete-trustpoint-action – Event delete trustpoint action message • export-trustpoint – Event export trustpoint message • import-trustpoint – Event import trustpoint message • rsa-key-actions-failure – Event RSA key actions failure message • rsa-key-actions-success – Event RSA key actions success message • svr-cert-actions-success – Event server certificate actions success message • svr-cert-actions-failure – Event server certificate actions failure message
cfgd	Configures configuration daemon module related event messages • acl-attached-altered – Event *Access List* (ACL) attached altered message • acl-rule-altered – Event ACL rule altered message
cluster	Configures cluster module related messages • cmaster-cfg-update-fail – Event cluster master config update failed message • max-exceeded – Event maximum cluster count exceeded message
crm	Configures *Critical Resource Monitoring* (CRM) related event messages • critical-resource-down – Event Critical Resource Down message • critical-resource-up – Event Critical Resource Up message
dhcpsvr	Configures DHCP server related event messages • dhcp-start – Event DHCP server started message • dhcpsvr-stop – Event DHCP sever stopped message • relay-iface-no-ip – Event no IP address on DHCP relay interface message • relay-no-iface – Event no interface for DHCP relay message • relay-start – Event relay agent started • relay-stop – Event DHCP relay agent stopped

<event-type>	<event-name>
diag	Configures diagnostics module related event messages • autogen-tech-sprt – Event autogen technical support message • buf-usage – Event buffer usage message • cpu-load – Event CPU load message • cpu-usage-too-high – Event CPU usage high message • cpu-usage-too-high-recovery – Event recovery from high CPU usage message • disk-usage – Event disk usage message • elapsed-time – Event elapsed time message • fan-underspeed – Event fan underspeed message • fd-count – Event forward count message • free-flash-disk – Event free flash disk message • free-flash-inodes – Event free flash inodes message • free-nvram-disk – Event free nvram disk message • free-nvram-inodes – Event free nvram inodes message • free-ram – Event free ram message • free-ram-disk – Event free ram disk message • free-ram-inodes – Event free ram inodes message • head-cache-usage – Event head cache usage message • high-temp – Event high temp message • ip-dest-usage – Event ip destination usage message • led-identify – Event led identify message • low-temp – Event low temp message • mem-usage-too-high – Event memory usage high message • mem-usage-too-high-recovery – Event recovery from high memory usage message • new-led-state – Event new led state message • over-temp – Event over temp message • over-voltage – Event over voltage message • poe-init-fail – Event PoE init fail message • poe-power-level – Event PoE power level message • poe-read-fail – Event PoE read fail message • poe-state-change – Event PoE state change message Contd..
	• poe-state-change – Event PoE state change message • pwrsply-fail – Event failure of power supply message • raid-degraded – Event *Redundant Array of Independent Disk*s (RAID) degraded message • raid-error – Event RAID error message • ram-usage – Event ram usage message • under-voltage – Event under voltage message • wd-reset-sys – Event wd reset system message • wd-state-change – Event wd state change message

<event-type>	<event-name>
dot11	Configures 802.11 management module related event messages • client-associated – Wireless client associated event message • client-denied-assoc – Event client denied association message • client-disassociated – Wireless client disassociated message • country-code – Event country code message • country-code-error – Event country code error message • eap-cached-keys – Event *Extensible Authentication Protocol* (EAP) cached keys message • eap-client-timeout – Event EAP client timeout message • eap-failed – Event EAP failed message • eap-opp-cached-keys – Event EAP opp cached keys message • eap-preauth-client-timeout – Event EAP pre authentication client timeout message • eap-preauth-failed – Event EAP pre authentication failed message • eap-preauth-server-timeout – Event EAP pre authentication server timeout message • eap-preauth-success – Event EAP pre authentication success message • eap-server-timeout – Event EAP server timeout message • eap-success – Event EAP success message • ft-roam-success – Event client fast BSS transition message • move-operation-success – Event move operation success message • neighbor-denied-assoc – Event neighbor denied association message • unsanctioned-br-active – Event unsanctioned AP active message • unsanctioned-br-inactive – Event unsanctioned AP inactive message • unsanctioned-br-status-change – Event unsanctioned AP status change • voice-call-completed – Event voice call completed message • voice-call-established – Event voice call established message • voice-call-failed – Event voice call failed message • wlan-time-access-disable – Event WLAN disabled by time-based-access message • wlan-time-access-enable – Event WLAN re-enabled by time-based-access message • wpa-wpa2-failed – Event WPA-WPA2 failed message • wpa-wpa2-key-rotn – Event WPA-WPA2 key rotn message • wpa-wpa2-success – Event WPA-WPA2 success message
dot1x	Configures 802.1X authentication related event messages • dot1x-failed – Event EAP authentication failure message • dot1x-success – Event dot1x-success message
fwu	Configures *firmware update* (fwu) related event messages • fwuaborted – Event fwu aborted message • fwubadconfig – Event fwu aborted due to bad config message • fwucorruptedfile – Event fwu aborted due to corrupted file message • fwucouldntgetfile – Event fwu aborted because the system could not get file message • fwudone – Event fwu done message • fwufileundef – Event fwu aborted due to file undefined message • fwunoneed – Event fwu no need message • fwuprodmismatch – Event fwu aborted due to product mismatch message • fwuserverundef – Event fwu aborted due to server undefined message • fwuserverunreachable – Event fwu aborted due to server unreachable message • fwusignmismatch – Event fwu aborted due to signature mismatch message • fwusyserr – Event fwu aborted due to system error message • fwuunsupportedhw – Event fwu aborted due to unsupported hardware message • fwuunsupportedmodelnum – Event fwu aborted due to unsupported FIPS model number message • fwuvermismatch – Event fwu aborted due to version mismatch message

<event-type>	<event-name>
isdn	Configures file *Integrated Service Digital Network* (ISDN) module related event messages • isdn-alert – Event ISDN alert message • isdn-crit – Event ISDN critical message • isdn-debug – Event ISDN debug message • isdn-emerg – Event ISDN emergency message • isdn-err – Event ISDN error message • isdn-info – Event ISDN info message • isdn-notice – Event ISDN notice message • isdn-warning – Event ISDN warning message
l2tpv3	Configures L2TPv3 related event messages • l2tpv3-tunnel-down – Event L2TPv3 tunnel down message • l2tpv3-tunnel-up – Event L2TPv3 tunnel up message
licmgr	Configures license manager module related event messages • lic-installed-count – Event total number of license installed count message • lic-installed-default – Event default license installation message • lic-installed – Event license installed message • lic-invalid – Event license installation failed message • lic-removed – Event license removed message
mgmt	Configures management services module related event messages • log-http-init – Event Web server started • log-http-local-start – Event Web server started in local mode • log-http-start – Event Web server started in external mode • log-https-start – Event secure Web server started • log-https-wait – Event waiting for Web server to start • log-key-deleted – Event RSA key associated with SSH is deleted • log-key-restored – Event RSA key associated with SSH is added • log-trustpoint-deleted – Event trustpoint associated with HTTPS is deleted
mesh	Configures mesh module related event messages • mesh-link-down – Event mesh link down message • mesh-link-up – Event mesh link up message • meshpoint-down – Event meshpoint down message • meshpoint-loop-prevent-off – Event meshpoint loop prevent off message • meshpoint-loop-prevent-on – Event meshpoint loop prevent on message • meshpoint-path-change – Event meshpoint-path-change message • meshpoint-root-change – Event meshpoint-root-change message • meshpoint-up – Event meshpoint up message

<event-type>	<event-name>
nsm	Configures *Network Service Module* (NSM) related event message • dhcpc-err – Event DHCP certification error message • dhcpdefrt – Event DHCP defrt message • dhcpip – Event DHCP IP message • dhcpipchg – Event DHCP IP change message • dhcpipnoadd – Event DHCP IP overlaps static IP address message • dhcplsexp – Event DHCP lease expiry message • dhcpnak – Event DHCP server returned DHCP NAK response • dhcpnodefrt – Event interface no default route message • if-failback – Event interface failback message • if-failover – EVENT Interface failover message • ifdown – Event interface down message • ifipcfg – Event interface IP config message • ifup – Event interface up message • nsm-ntp – Event translate host name message
pm	Configures process monitor module related event messages • procid – Event proc ID message • procmaxrstrt – Event proc max restart message • procnoresp – Event proc no response message • procrstrt – Event proc restart message • procstart – Event proc start message • procstop – Event proc stop message • procsysrstrt – Event proc system restart message • startupcomplete – Event startup complete message
radconf	Configures RADIUS configuration daemon related event messages • could-not-stop-radius – Event could not stop RADIUS server message • radiusdstart – Event RADIUS server started message • radiusdstop – Event RADIUS server stopped message
radio	Configures radio module related event messages • acs-scan-complete – Event ACS scan completed • acs-scan-started – Event ACS scan started • channel-country-mismatch – Event channel and country of operation mismatch message • radar-det-info – Detected radar info message • radar-detected – Event radar detected message • radar-scan-completed – Event radar scan completed message • radar-scan-started – Event radar scan started message • radio-antenna-error – Event invalid antenna type on this radio message • radio-antenna-setting – Event antenna type setting on this radio message • radio-state-change – Event radio state change message • resume-home-channel – Event resume home channel message
smrt	Configures SMART RF module related event messages • calibration-done – Event calibration done message • calibration-started – Event calibration started message • channel-change – Event channel change message • config-cleared – Configuration cleared event message • cov-hole-recovery – Event coverage hole recovery message • cov-hole-recovery-done – Event coverage hole recovery done message • interference-recovery – Event interference recovery message • neighbor-recovery – Event neighbor recovery message • power-adjustment – Event power adjustment message • root-recovery – Event meshpoint root recovery message

<event-type>	<event-name>
smtpnot	Configures SMTP module related event messages • cfg – Event cfg message • cfginc – Event cfg inc message • net – Event net message • proto – Event proto message • smtpauth – Event SMTP authentication message • smtperr – Event SMTP error message • smtpinfo – Event SMTP information message
system	Configures system module related event messages • clock-reset – Event clock reset message • cold-start – Event cold start message • config-commit – Event configuration commit message • guest-user-exp – Event guest user purging message • http-err – Event Web server did not start message • login – Event successful login message • login-fail – Event login fail message. Occurs when user authentication fails. • login-fail-access – Event login fail access message. Occurs in case of access violation. • login-fail-bad-role – Event login fail bad role message. Occurs when user uses an invalid role to logon. • logout – Event logout message • maat-light – Event action on *Research in Motion* (RIM) radio(s) from the Maat light module • panic – Event panic message • periodic-heart-beat – Event periodic heart beat message • procstop – Event proc stop message • server-unreachable – Event server-unreachable message • system-autoup-disable – Event system autoup disable message • system-autoup-enable – Event system autoup enable message • ui-user-auth-fail – Event user authentication fail message • ui-user-auth-success – Event user authentication success message • warm-start – Event warm start message • warm-start-recover – Event recovery from warm start message
test	Configures the test module related event messages • testalert – Event test alert message • testargs – Event test arguments message • testcrit – Event test critical message • testdebug – Event test debug message • testemerg – Event test emergency message • testerr – Event test error message • testinfo – Event test information message • testnotice – Event test notice message • testwarn – Event test warning message
vrrp	Configures *Virtual Router Redundancy Protocol* (VRRP) related event messages • vrrp-monitor-change – Event VRRP monitor link state change message • vrrp-state-change – Event VRRP state transition message • vrrp-vip-subnet-mismatch – Event VRRP IP not overlapping with an interface addresses message
wips	Configures the Wireless IPS module related event messages • wips-client-blacklisted – Event WIPS client blacklisted message • wips-client-rem-blacklist – Event WIPS client rem blacklist message • wips-event – Event WIPS event triggered message
email	Sends e-mail notifications to a pre configured e-mail ID
forward-to-switch	Forwards the messages to an external server

<event-type>	<event-name>
snmp	Logs an SNMP event
syslog	Logs an event to syslog
default	Performs the default action for the event
off	Switches the event off, when the event happens, and no action is performed
on	Switches the event on, when the event happens, and the configured action is taken

Example

```
rfs7000-37FABE(config-event-system-policy-event-testpolicy)#event aaa
radius-discon-msg email on forward-to-switch default snmp default syslog
default
rfs7000-37FABE(config-event-system-policy-event-testpolicy)#

rfs7000-37FABE(config-event-system-policy-testpolicy)#show context
event-system-policy test
 event aaa radius-discon-msg email on
rfs7000-37FABE(config-event-system-policy-testpolicy)#
```

Related Commands:

no	Resets or disables event monitoring

no

event-system-policy-mode commands

Negates an event monitoring configuration

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no event <EVENT-TYPE> <EVENT-NAME> [email|forward-to-switch|snmp|syslog]
          [default|on|off]
```

Parameters

```
no event <EVENT-TYPE> <EVENT-NAME> [email|forward-to-switch|snmp|syslog]
[default|on|off]
```

no event <EVENT-TYPE> <EVENT-NAME>	Removes the specified event monitoring activity • <EVENT-TYPE> – Select the event type. • <EVENT-NAME> – After selecting the event type, specify the event name. **NOTE:** The system stops network monitoring for the occurrence of the specified event and no notification is sent if the event occurs.

Example

```
rfs7000-37FABE(config-event-system-policy-TestPolicy)#event br adopted syslog
default
rfs7000-37FABE(config-event-system-policy-TestPolicy)#

rfs7000-37FABE(config-event-system-policy-TestPolicy)#no event br adopted
syslog
rfs7000-37FABE(config-event-system-policy-TestPolicy)#
```

Related Commands:

event	Configures the action taken for each event

firewall-policy

Global Configuration Commands

Configures a firewall policy. This policy defines a set of rules for managing network traffic and prevents unauthorized access to the network behind the firewall.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
firewall-policy <FIREWALL-POLICY-NAME>
```

Parameters

```
firewall-policy <FIREWALL-POLICY-NAME>
```

<FIREWALL-POLICY-NAME>	Specify the firewall policy name. If a firewall policy does not exist, it is created.

Example

```
rfs7000-37FABE(config)#firewall-policy test
rfs7000-37FABE(config-fw-policy-test)#?
Firewall policy Mode commands:
  acl-logging                   Log on flow creating traffic
  alg                           Enable ALG
  clamp                         Clamp value
  dhcp-offer-convert            Enable conversion of broadcast dhcp offers to
                                unicast
  dns-snoop                     DNS Snooping
  firewall                      Wireless firewall
  flow                          Firewall flow
  ip                            Internet Protocol (IP)
  ip-mac                        Action based on ip-mac table
  logging                       Firewall enhanced logging
  no                            Negate a command or set its defaults
  proxy-arp                     Enable generation of ARP responses on behalf
                                of another device
```

```
  stateful-packet-inspection-l2  Enable stateful packet inspection in layer2
                                 firewall
  storm-control                  Storm-control
  virtual-defragmentation        Enable virtual defragmentation for IPv4
                                 packets (recommended for proper functioning
                                 of firewall)

  clrscr                         Clears the display screen
  commit                         Commit all changes made in this session
  do                             Run commands from Exec mode
  end                            End current mode and change to EXEC mode
  exit                           End current mode and down to previous mode
  help                           Description of the interactive help system
  revert                         Revert changes
  service                        Service Commands
  show                           Show running system information
  write                          Write running configuration to memory or
                                 terminal

rfs7000-37FABE(config-fw-policy-test)#
```

Related Commands:

no	Removes an existing firewall policy

NOTE
For more information on Firewall policy, see *Chapter 14, FIREWALL-POLICY*.

global-association-list

Global Configuration Commands

Configures a global list of client MAC addresses. Based on the deny or permit rules specified, clients are either allowed or denied access to the managed network.

The global association list serves the same purpose as an Association *Access Control List* (ACL). However, the Association ACL allows a limited number of entries, a few thousand only, and does not suffice the requirements of a large deployment. This gap is filled by a global association list, which is much larger (with tens of thousands of entries). Both lists co-exist in the system. When an access request comes in, the association ACL is looked up first and if the requesting MAC address is listed in one of the deny ACLs, the association is denied. But, if the requesting client is permitted access, or if in case none of the ACLs list the client's MAC address, the global association ACL is checked. Once authenticated, the client's credentials are cached on the access point, and subsequent requests are not referenced to the controller. An entry in an APs credential cache means a pass in the global association list.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
global-association-list <GLOBAL-ASSOC-LIST-NAME>
```

Parameters

```
global-association-list <GLOBAL-ASSOC-LIST-NAME>
```

<GLOBAL-ASSOC-LIST-NAME>	Specify the global association list name. If a list with the same name does not exist, it is created. Map this global association list to a device (controller) or a controller profile.Once associated, the controller applies this association list to requests received from all adopted APs. For more information, see *use*. The global association list can also be mapped to a WLAN. The usage of global access lists is controlled on a per-WLAN basis. For more information, see *association-list*.

Example

```
rfs4000-229D58(config)#global-association-list my-clients
rfs4000-229D58(config-global-assoc-list-my-clients)#?
Global Association List Mode commands:
  default-action  Configure the default action when the client MAC does not
                  match any rule
  deny            Specify MAC addresses to be denied
  no              Negate a command or set its defaults
  permit          Specify MAC addresses to be permitted

  clrscr          Clears the display screen
  commit          Commit all changes made in this session
  do              Run commands from Exec mode
  end             End current mode and change to EXEC mode
  exit            End current mode and down to previous mode
  help            Description of the interactive help system
  revert          Revert changes
  service         Service Commands
  show            Show running system information
  write           Write running configuration to memory or terminal

rfs4000-229D58(config-global-assoc-list-my-clients)#

rfs4000-229D58(config-global-assoc-list-my-clients)#permit 00-23-69-11-E6-C4
desc
ription "10th floor Lab1 Workstation1"
rfs4000-229D58(config-global-assoc-list-my-clients)#

rfs4000-229D58(config-global-assoc-list-my-clients)#show context
global-association-list my-clients
 permit 00-23-69-11-E6-C4 description "10th floor Lab1 Workstation1"
rfs4000-229D58(config-global-assoc-list-my-clients)#
rfs4000-229D58(config)#show context
!
! Configuration of Brocade Mobility RFS4000 version 5.5.0.0-042B
!
!
version 2.3
!
!
client-identity TestClientIdentity
 dhcp 1 message-type request option-codes exact hexstring 5e4d36780b3a7f
!
client-identity-group ClientIdentityGroup
 client-identity TestClientIdentity precedence 1
!
```

```
ip access-list BROADCAST-MULTICAST-CONTROL
.....................................................................
global-association-list my-clients
 permit 00-23-69-11-E6-C4 description "10th floor Lab1 Workstation1"
!
global-association-list test
 permit 11-22-33-44-55-66 description test
 deny 22-33-44-55-66-77 description "Test Deny"
!
captive-portal test
--More--
rfs4000-229D58(config)#

rfs4000-229D58(config-device-00-23-68-22-9D-58)#use global-assoc-list server
my-
clients
rfs4000-229D58(config-device-00-23-68-22-9D-58)#

rfs4000-229D58(config-device-00-23-68-22-9D-58)#show context
rfs4000 00-23-68-22-9D-58
 use profile default-rfs4000
 use rf-domain default
 hostname rfs4000-229D58
 license AP DEFAULT-6AP-LICENSE
 license ADSEC DEFAULT-ADV-SEC-LICENSE
 ip default-gateway 192.168.13.2
 ip default-gateway priority static-route 20
 interface ge1
  switchport mode access
  switchport access vlan 1
 interface vlan1
  ip address 192.168.13.9/24
  ip address 192.168.0.1/24 secondary
  ip dhcp client request options all
 use global-association-list server my-clients
 use client-identity-group ClientIdentityGroup
 logging on
 logging console warnings
 logging buffered warnings
rfs4000-229D58(config-device-00-23-68-22-9D-58)#
```

host

Global Configuration Commands

Enters the configuration context of a remote device using its hostname

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
host <DEVICE-NAME>
```

Parameters

```
host <DEVICE-NAME>
```

<DEVICE-NAME>	Specify the device's hostname. All discovered devices are displayed when 'Tab' is pressed to auto complete this command.

Example

```
rfs7000-37FABE(config)#host rfs7000-37FABE
rfs7000-37FABE(config-device-00-04-96-42-14-79)#
```

inline-password-encryption

Global Configuration Commands

Stores the encryption key in the startup configuration file

By default, the encryption key is not stored in the startup-config file. Use the inline-password-encryption command to move the encrypted key to the startup-config file. This command uses the master key to encrypt the password, then moves it to the startup-config file.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
inline-password-encryption
```

Parameters

None

Usage Guidelines:

When the configuration file is imported to a different device, it first decrypts the encryption key using the default key and then decrypts the rest of the configuration using the administrator configured encryption key.

Example

```
rfs7000-37FABE(config)#password-encryption secret 2 12345678
rfs7000-37FABEconfig)#

rfs7000-37FABE(config)#commit wr mem
rfs7000-37FABE(config)#

This command uses the specified password for encryption key and stores it
outside of startup-config

rfs7000-37FABE(config)#inline-password-encryption
rfs7000-37FABE(config)#
```

```
This command moves the same password to the startup-config and encrypts it
with the master key.
```

Related Commands:

no	Disables storing of the encryption key in the startup configuration file

ip

Global Configuration Commands

Configures IP access control lists

Access lists define access permissions to the network using a set of rules. Each rule specifies an action taken when a packet matches the rule. If the action is deny, the packet is dropped. If the action is permit, the packet is allowed.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
ip access-list <IP-ACCESS-LIST-NAME>
```

Parameters

```
ip access-list <IP-ACCESS-LIST-NAME>
```

access-list <IP-ACCESS-LIST-NAME>	Configures an IP access list • <IP-ACCESS-LIST-NAME> – Specify the ACL name. If the access list does not exist, it is created.

Example

```
rfs7000-37FABE(config)#ip access-list test

rfs7000-37FABE(config-ip-acl-test)#?
ACL Configuration commands:
  deny     Specify packets to reject
  disable  Disable rule if not needed
  no       Negate a command or set its defaults
  permit   Specify packets to forward

  clrscr   Clears the display screen
  commit   Commit all changes made in this session
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  revert   Revert changes
  service  Service Commands
  show     Show running system information
  write    Write running configuration to memory or terminal
```

```
rfs7000-37FABE(config-ip-acl-test)#
```

Related Commands:

no	Removes an IP access control list

NOTE
For more information on Access Control Lists, see *Chapter 12, ACCESS-LIST*.

l2tpv3

Global Configuration Commands

Configures a *Layer 2 Tunnel Protocol Version 3* (L2TPv3) tunnel policy, used to create one or more L2TPv3 tunnels.

The L2TPv3 policy defines the control and encapsulation protocols needed for tunneling layer 2 frames between two IP nodes. This policy enables creation of L2TPv3 tunnels for transporting Ethernet frames between bridge VLANs and physical GE ports. L2TPv3 tunnels can be created between any vendor devices supporting L2TPv3 protocol.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
l2tpv3 policy <L2TPV3-POLICY-NAME>
```

Parameters

```
l2tpv3 policy <L2TPV3-POLICY-NAME>
```

l2tpv3 policy <L2TPV3-POLICY-NAME>	Configures an L2TPv3 tunnel policy • <L2TPV3-POLICY-NAME> – Specify a policy name. The policy is created if it does not exist. To modify an existing L2TPv3, specify its name.

Example

```
rfs7000-37FABE(config)#l2tpv3 policy L2TPV3Policy1
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#?
L2tpv3 Policy Mode commands:
  cookie-size             Size of the cookie field present in each l2tpv3 data
                          message
  failover-delay          Time interval for re-establishing the tunnel after
                          the failover (RF-Domain
                          manager/VRRP-master/Cluster-master failover)
  force-l2-path-recovery  Enables force learning of servers, gateways etc.,
                          behind the l2tpv3 tunnel when the tunnel is
                          established
  hello-interval          Configure the time interval (in seconds) between
                          l2tpv3 Hello keep-alive messages exchanged in l2tpv3
```

```
                          control connection
  no                      Negate a command or set its defaults
  reconnect-attempts      Maximum number of attempts to reestablish the
                          tunnel.
  reconnect-interval      Time interval between the successive attempts to
                          reestablish the l2tpv3 tunnel
  retry-attempts          Configure the maximum number of retransmissions for
                          signaling message
  retry-interval          Time interval (in seconds) before the initiating a
                          retransmission of any l2tpv3 signaling message
  rx-window-size          Number of signaling messages that can be received
                          without sending the acknowledgement
  tx-window-size          Number of signaling messages that can be sent
                          without receiving the acknowledgement

  clrscr                  Clears the display screen
  commit                  Commit all changes made in this session
  end                     End current mode and change to EXEC mode
  exit                    End current mode and down to previous mode
  help                    Description of the interactive help system
  revert                  Revert changes
  service                 Service Commands
  show                    Show running system information
  write                   Write running configuration to memory or terminal

rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#
```

Related Commands:

no	Removes an existing L2TPv3 tunnel policy
mint-policy	Configures the global MiNT policy

NOTE
For more information on the L2TPv3 tunnel configuration mode and commands, see *Chapter 23, L2TPV3-POLICY*.

mac

Global Configuration Commands

Configures MAC access control lists

Access lists define access permissions to the network using a set of rules. Each rule specifies an action taken when a packet matches the rule. If the action is deny, the packet is dropped. If the action is permit, the packet is allowed.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
mac access-list <MAC-ACCESS-LIST-NAME>
```

Parameters

```
mac access-list <MAC-ACCESS-LIST-NAME>
```

access-list <IP-ACCESS-LIST-NAME>	Configures a MAC access control list • <MAC-ACCESS-LIST-NAME> – Specify the ACL name. If the access control list does not exist, it is created.

Example

```
rfs7000-37FABE(config)#mac access-list test

rfs7000-37FABE(config-mac-acl-test)#?
MAC Extended ACL Configuration commands:
  deny     Specify packets to reject
  disable  Disable rule if not needed
  no       Negate a command or set its defaults
  permit   Specify packets to forward

  clrscr   Clears the display screen
  commit   Commit all changes made in this session
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  revert   Revert changes
  service  Service Commands
  show     Show running system information
  write    Write running configuration to memory or terminal

rfs7000-37FABE(config-mac-acl-test)#
```

Related Commands:

no	Removes a MAC access control list

NOTE
For more information on Access Control Lists, see *Chapter 12, ACCESS-LIST*.

management-policy

Global Configuration Commands

Configures a management policy. Management policies include services that run on a device, welcome messages, banners etc.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
management-policy <MANAGEMENT-POLICY-NAME>
```

Parameters

```
management-policy <MANAGEMENT-POLICY-NAME>
```

<MANAGEMENT-POLICY-NAME>	Specify the management policy name. If the policy does not exist, it is created.

Example

```
rfs7000-37FABE(config)#management-policy test
rfs7000-37FABE(config-management-policy-test)#?
Management Mode commands:
  aaa-login                Set authentication for logins
  banner                   Define a login banner
  ftp                      Enable FTP server
  http                     Hyper Text Terminal Protocol (HTTP)
  https                    Secure HTTP
  idle-session-timeout     Configure idle timeout for a configuration session
                           (GUI or CLI)
  no                       Negate a command or set its defaults
  privilege-mode-password  Set the password for entering CLI privilege mode
  restrict-access          Restrict management access to the device
  snmp-server              SNMP
  ssh                      Enable ssh
  telnet                   Enable telnet
  user                     Add a user account

  clrscr                   Clears the display screen
  commit                   Commit all changes made in this session
  do                       Run commands from Exec mode
  end                      End current mode and change to EXEC mode
  exit                     End current mode and down to previous mode
  help                     Description of the interactive help system
  revert                   Revert changes
  service                  Service Commands
  show                     Show running system information
  write                    Write running configuration to memory or terminal

rfs7000-37FABE(config-management-policy-test)#
```

Related Commands:

no	Removes an existing management policy

NOTE
For more information on Management policy configuration, see *Chapter 16, MANAGEMENT-POLICY*.

meshpoint

Global Configuration Commands

Creates a new meshpoint and enters its configuration mode. Use this command to select and configure existing meshpoints.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
meshpoint [<MESHPOINT-NAME>|containing <WORD>]
```

Parameters

```
meshpoint [<MESHPOINT-NAME>|containing <WORD>]
```

<MESHPOINT-NAME>	Specify the meshpoint name. If the meshpoint does not exist, it is created.
containing <WORD>	Selects existing meshpoints containing the sub-string <WORD> in their names

Example

```
rfs7000-37FABE(config)#meshpoint TestMeshpoint
rfs7000-37FABE(config-meshpoint-TestMeshpoint)#?
Mesh Point Mode commands:
  allowed-vlans  Set the allowed VLANs
  beacon-format  The beacon format of this meshpoint
  control-vlan   VLAN for meshpoint control traffic
  data-rates     Specify the 802.11 rates to be supported on this meshpoint
  description    Configure a description of the usage of this meshpoint
  meshid         Configure the Service Set Identifier for this meshpoint
  neighbor       Configure neighbor specific parameters
  no             Negate a command or set its defaults
  root           Set this meshpoint as root
  security-mode  The security mode of this meshpoint
  shutdown       Shutdown this meshpoint
  use            Set setting to use
  wpa2           Modify ccmp wpa2 related parameters

  clrscr         Clears the display screen
  commit         Commit all changes made in this session
  do             Run commands from Exec mode
  end            End current mode and change to EXEC mode
  exit           End current mode and down to previous mode
  help           Description of the interactive help system
  revert         Revert changes
  service        Service Commands
  show           Show running system information
  write          Write running configuration to memory or terminal

rfs7000-37FABE(config-meshpoint-TestMeshpoint)#
```

Related Commands:

no	Removes an existing meshpoint

NOTE
For more information on Meshpoint configuration, see *Chapter 27, MESHPOINT*

meshpoint-qos-policy

Global Configuration Commands

Configures a set of parameters that defines the meshpoint *quality of service* (QoS) policy

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
meshpoint-qos-policy <MESHPOINT-QOS-POLICY-NAME>
```

Parameters

```
meshpoint-qos-policy <MESHPOINT-QOS-POLICY-NAME>
```

<MESHPOINT-QOS-POLICY-NAME>	Specify the meshpoint QoS policy name. If the policy does not exist, it is created.

Example

```
rfs7000-37FABE(config)#meshpoint-qos-policy TestMeshpointQoS
rfs7000-37FABE(config-meshpoint-qos-TestMeshpointQoS)#?
Mesh Point QoS Mode commands:
  accelerated-multicast  Configure accelerated multicast streams address and
                         forwarding QoS classification
  no                     Negate a command or set its defaults
  rate-limit             Configure traffic rate-limiting parameters on a
                         per-meshpoint/per-neighbor basis

  clrscr                 Clears the display screen
  commit                 Commit all changes made in this session
  do                     Run commands from Exec mode
  end                    End current mode and change to EXEC mode
  exit                   End current mode and down to previous mode
  help                   Description of the interactive help system
  revert                 Revert changes
  service                Service Commands
  show                   Show running system information
  write                  Write running configuration to memory or terminal

rfs7000-37FABE(config-meshpoint-qos-TestMeshpointQoS)#
```

Related Commands:

no	Removes an existing meshpoint QoS policy

NOTE
For more information on meshpoint QoS policy configuration, see *Chapter 27, MESHPOINT*

mint-policy

Global Configuration Commands

Configures the global MiNT policy

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
mint-policy global-default
```

Parameters

```
mint-policy global-default
```

global-default	Uses the global default MiNT policy

Example

```
rfs7000-37FABE(config)#mint-policy global-default
rfs7000-37FABE(config-mint-policy-global-default)#?
Mint Policy Mode commands:
  level    Mint routing level
  mtu      Configure the global Mint MTU
  no       Negate a command or set its defaults
  router   Mint router
  udp      Configure mint UDP/IP encapsulation

  clrscr   Clears the display screen
  commit   Commit all changes made in this session
  do       Run commands from Exec mode
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  revert   Revert changes
  service  Service Commands
  show     Show running system information
  write    Write running configuration to memory or terminal

rfs7000-37FABE(config-mint-policy-global-default)#
```

Related Commands:

no	Removes an existing MiNT policy

NOTE
For more information on MiNT policy configuration, see *Chapter 15, MINT-POLICY*.

nac-list

Global Configuration Commands

A *Network Access Control* (NAC) policy configures a list of devices that can access a network based on their MAC addresses.

The following table lists NAC list configuration mode commands.

Command	Description	Reference
nac-list	Creates a NAC list and enters its configuration mode	page 259
nac-list-mode commands	Summarizes NAC list configuration mode commands	page 260

nac-list

nac-list

Configures a NAC list that manages access to the network

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
nac-list <NAC-LIST-NAME>
```

Parameters

```
nac-list <NAC-LIST-NAME>
```

<NAC-LIST-NAME>	Specify the NAC list name. If the NAC list does not exist, it is created.

Example

```
rfs7000-37FABE(config)#nac-list test
rfs7000-37FABE(config-nac-list-test)#?
NAC List Mode commands:
  exclude  Specify MAC addresses to be excluded from the NAC enforcement list
  include  Specify MAC addresses to be included in the NAC enforcement list
  no       Negate a command or set its defaults

  clrscr   Clears the display screen
  commit   Commit all changes made in this session
  do       Run commands from Exec mode
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
```

```
  help     Description of the interactive help system
  revert   Revert changes
  service  Service Commands
  show     Show running system information
  write    Write running configuration to memory or terminal

rfs7000-37FABE(config-nac-list-test)#
```

Related Commands:

no	Removes a NAC list

nac-list-mode commands

nac-list

The following table summarizes NAC list configuration mode commands.

Command	Description	Reference
exclude	Specifies the MAC addresses excluded from the NAC enforcement list	page 260
include	Specifies the MAC addresses included in the NAC enforcement list	page 261
no	Cancels an exclude or include NAC list rule	page 262
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

exclude

nac-list-mode commands

Specifies the MAC addresses excluded from the NAC enforcement list

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
exclude <START-MAC> [<END-MAC> precedence <1-1000>|precedence <1-1000>]
```

Parameters

```
exclude <START-MAC> [<END-MAC> precedence <1-1000>|precedence <1-1000>]
```

<START-MAC>	Specifies a range of MAC addresses or a single MAC address to exclude from the NAC enforcement list • <START-MAC> – Specify the first MAC address in the range. **NOTE:** Use this parameter to specify a single MAC address.
<END-MAC>	Specifies the last MAC address in the range (optional if a single MAC is added to the list) • <END-MAC> – Specify the last MAC address in the range.
precedence <1-1000>	Sets the rule precedence. Exclude entries are checked in the order of their rule precedence. • <1-1000> – Specify a value from 1 - 1000.

Example

```
rfs7000-37FABE(config-nac-list-test)#exclude 00-40-96-B0-BA-2A precedence 1

rfs7000-37FABE(config-nac-list-test)#show context
nac-list test
 exclude 00-40-96-B0-BA-2A 00-40-96-B0-BA-2A precedence 1
rfs7000-37FABE(config-nac-list-test)#
```

include

nac-list-mode commands

Specifies the MAC addresses included in the NAC enforcement list

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
include <START-MAC> [<END-MAC> precedence <1-1000>|precedence <1-1000>]
```

Parameters

```
include <START-MAC> [<END-MAC> precedence <1-1000>|precedence <1-1000>]
```

<START-MAC>	Specifies a range of MAC addresses or a single MAC address to include in the NAC enforcement list • <START-MAC> – Specify the first MAC address in the range. **NOTE:** Use this parameter to specify a single MAC address
<END-MAC>	Specifies the last MAC address in the range (optional if a single MAC is added to the list) • <END-MAC> – Specify the last MAC address in the range.
precedence <1-1000>	Sets the rule precedence. Exclude entries are checked in the order of their rule precedence. • <1-1000> – Specify a value from 1 - 1000.

Example

```
rfs7000-37FABE(config-nac-list-test)#include 00-15-70-38-06-49 precedence 2

rfs7000-37FABE(config-nac-list-test)#show context
nac-list test
```

```
 exclude 00-04-96-B0-BA-2A 00-04-96-B0-BA-2A precedence 1
 include 00-15-70-38-06-49 00-15-70-38-06-49 precedence 2
rfs7000-37FABE(config-nac-list-test)#
```

no

nac-list-mode commands

Cancels an exclude or include NAC list rule

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no [exclude|include]

no [exclude|include] <START-MAC> [<END-MAC> precedence <1-1000>|precedence
<1-1000>]
```

Parameters

```
no [exclude|include] <START-MAC> [<END-MAC> precedence <1-1000>|precedence
<1-1000>]
```

no exclude	Removes an exclude rule
no include	Removes an include rule
<START-MAC>	Specifies a range of MACs included in/removed from the NAC enforcement list Specify the first MAC address in the range. **NOTE:** Use this parameter to specify a single MAC address.
<END-MAC>	Specify the last MAC address in the range (optional if a single MAC is added to the list).
precedence <1-1000>	Sets the rule precedence for this rule. Exclude entries are checked in the order of their rule precedence. • <1-1000> – Specify a value from 1 - 1000.

Example

```
The following example shows the NAC list ‘test’ settings before the ‘no’
command is executed:

rfs7000-37FABE(config-nac-list-test)#show context
nac-list test
 exclude 00-04-96-B0-BA-2A 00-04-96-B0-BA-2A precedence 1
 include 00-15-70-38-06-49 00-15-70-38-06-49 precedence 2
rfs7000-37FABE(config-nac-list-test)#

rfs7000-37FABE(config-nac-list-test)#no exclude 00-40-96-B0-BA-2A precedence 1

The following example shows the NAC list ‘test’ settings after the ‘no’
command is executed:

rfs7000-37FABE(config-nac-list-test)#show context
```

```
nac-list test
 include 00-15-70-38-06-49 00-15-70-38-06-49 precedence 2
rfs7000-37FABE(config-nac-list-test)#
```

Related Commands:

exclude	Specifies MAC addresses excluded from the NAC enforcement list
include	Specifies MAC addresses included in the NAC enforcement list

no

Global Configuration Commands

Negates a command, or reverts configured settings to their default

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no
[aaa-policy|aaa-tacacs-policy|advanced-wips-policy|alias|br650|br6511|br1220|
br71xx|br81xx|association-acl-policy|auto-provisioning-policy|captive-portal|
client-identity|client-identity-group|customize|device|device-categorization|
dhcp-server-policy|dns-whitelist|event-system-policy|firewall-policy|global-a
ssociation-list|igmp-snoop-policy|inline-password-encryption|ip|l2tpv3|mac|ma
nagement-policy|meshpoint|meshpoint-qos-policy|nac-list|passpoint-policy|pass
word-encryption|profile|radio-qos-policy|radius-group|radius-server-policy|ra
dius-user-pool-policy|rf-domain|rfs4000|rfs6000|rfs7000|role-policy|routing-p
olicy|smart-rf-policy|wips-policy|wlan|wlan-qos-policy|service]

no alias [address-range <ADDRESS-RANGE-ALIAS-NAME>|host
<HOST-ALIAS-NAME>|network <NETWORK-ALIAS-NAME>|network-group
<NETWORK-GROUP-ALIAS-NAME> [address-range|host|network]|network-service
<NETWORK-SEVICE-ALIAS-NAME>|vlan <VLAN-ALIAS-NAME>]

no
[aaa-policy|aaa-tacacs-policy|advanced-wips-policy|auto-provisioning-policy|c
aptive-portal|device-categorization|dhcp-server-policy|dns-whitelist|event-sy
stem-policy|firewall-policy|global-association-list|inline-password-encryptio
n|ip|l2tpv3|mac|management-policy|meshpoint|meshpoint-qos-policy|nac-list|pas
spoint-policy|radio-qos-policy|radius-group|radius-server-policy|radius-user-
pool-policy|role-policy|routing-policy|smart-rf-policy|wips-policy|wlan-qos-p
olicy]

no [br650|br6511|br1220|br71xx|br81xx|rfs4000|rfs6000|rfs7000]

no client-identity <CLIENT-IDENTITY-NAME>

no client-identity-group <CLIENT-IDENTITY-GROUP-NAME>
```

```
no device {containing <WORD>} {(filter type
[br650|br6511|br1220|br71xx|br81xx])}

no customize
[hostname-column-width|show-wireless-client|show-wireless-client-stats|

show-wireless-client-stats-rf|show-wireless-meshpoint|show-wireless-meshpoint
-

neighbor-stats|show-wireless-meshpoint-neighbor-stats-rf|show-wireless-radio|
          show-wireless-radio-stats|show-wireless-radio-stats-rf]

no password-encryption secret 2 <OLD-PASSPHRASE>

no profile {br650|br6511|br1220|br71xx|br81xx|
          containing|filter}

no wlan [<WLAN-NAME>|all|containing <WLAN-NAME-SUBSTRING>]

no service set [command-history|reboot-history|upgrade-history] {on
<DEVICE-NAME>}
```

Parameters

```
no
[aaa-policy|aaa-tacacs-policy|advanced-wips-policy|auto-provisioning-policy|
captive-portal|device-categorization|dhcp-server-policy|dns-whitelist|event-s
ystem-policy|firewall-policy|global-association-policy|inline-password-encryp
tion|ip|
l2tpv3|mac|management-policy|meshpoint|meshpoint-qos-policy|nac-list|passpoin
t-policy|
radio-qos-policy|radius-group|radius-server-policy|radius-user-pool-policy|ro
le-policy|
routing-policy|smart-rf-policy|wips-policy|wlan-qos-policy]
```

no aaa-policy <POLICY-NAME>	Deletes the specified AAA policy
no aaa-tacacs-policy <POLICY-NAME>	Deletes the specified AAA TACACS policy
no advanced-wips-policy <POLICY-NAME>	Deletes the specified advanced WIPS policy
no auto-provisioning-policy <POLICY-NAME>	Deletes the specified auto provisioning policy
no captive-portal <CAPTIVE-PORTAL-NAME>	Deletes the specified captive portal
no device-categorization <DEVICE-CATEGORIZATION-LIST-NAME>	Deletes the specified device categorization list
no dhcp-server-policy <POLICY-NAME>	Deletes the specified DHCP server policy
no dns-whitelist <DNS-WHITELIST-NAME>	Deletes the specified DNS Whitelist
no event-system-policy <POLICY-NAME>	Deletes the specified event system policy

no firewall-policy <POLICY-NAME>	Deletes the specified firewall policy
no global-association-policy <POLICY-NAME>	Deletes the specified global association policy
no inline-password-encryption	Disables storing of the encryption key in the startup configuration file
no ip access-list <IP-ACCESS-LIST-NAME>	Deletes the specified IP access list
no l2tpv3 policy <L2TPV3-POLICY-NAME>	Deletes the specified L2TPv3 policy **NOTE:** The default L2TPv3 policy cannot be deleted.
no mac access-list <MAC-ACCESS-LIST-NAME>	Deletes the specified MAC access list
no management-policy <POLICY-NAME>	Deletes the specified management policy
no meshpoint <MESHPOINT-NAME>	Deletes the specified meshpoint
no meshpoint-qos-policy <POLICY-NAME>	Deletes the specified meshpoint QoS policy
no nac-list <NAC-LIST-NAME>	Deletes the specified NAC list
no passpoint-policy <POLICY-NAME>	Deletes the specified passpoint policy
no radio-qos-policy <POLICY-NAME>	Deletes the specified radio QoS policy
no radius-group <RADIUS-GROUP-NAME>	Deletes the specified RADIUS group
no radius-server-policy <POLICY-NAME>	Deletes the specified RADIUS server policy
no radius-user-pool-policy <POLICY-NAME>	Deletes the specified RADIUS user pool policy
no rf-domain <RF-DOMAIN-NAME>	Deletes the specified RF Domain
no role-policy <POLICY-NAME>	Deletes the specified role policy
no routing-policy <POLICY-NAME>	Deletes the specified routing policy
no smart-rf-policy <POLICY-NAME>	Deletes the specified smart RF policy
no wips-policy <POLICY-NAME>	Deletes the specified WIPS policy
no wlan-qos-policy <POLICY-NAME>	Deletes the specified WLAN QoS policy

```
no alias [address-range <ADDRESS-RANGE-ALIAS-NAME>|host <HOST-ALIAS-NAME>|
network <NETWORK-ALIAS-NAME>|network-group <NETWORK-GROUP-ALIAS-NAME>
[address-range|host|network]|network-service <NETWORK-SEVICE-ALIAS-NAME>|
vlan <VLAN-ALIAS-NAME>]
```

no alias	Removes an existing network, VLAN, or service alias. Select the alias type. The options are: network, vlan, and service.
address-range <ADDRESS-RANGE-ALIAS-NAME>	Deletes the specified address range alias
host <HOST-ALIAS-NAME>	Deletes the specified host alias
network <NETWORK-ALIAS-NAME>	Deletes the specified network alias
network-group <NETWORK-GROUP-ALIAS-NAME>	Removes the specified component (IP address(es), hosts, or network address(es)) of the specified network-group alias
network-service <NETWORK-SERVICE-ALIAS-NAME>	Deletes the specified network-service alias
vlan <VLAN-ALIAS-NAME>	Removes the VLAN alias identified by the <VLAN-ALIAS-NAME> keyword

```
no [|br650|br6511|br1220|br71xx|br81xx|rfs4000|rfs6000|rfs7000] <MAC>
```

no br650	Removes an Brocade Mobility 650 Access Point from the network
no br6511	Removes an Brocade Mobility 6511 Access Point from the network
no br1220	Removes an Brocade Mobility 1220 Access Point from the network
no br71xx	Removes an Brocade Mobility 71XX Access Point from the network
no rfs4000	Removes a Brocade Mobility RFS4000 from the network
no rfs6000	Removes a Brocade Mobility RFS6000 from the network
no rfs7000	Removes a Brocade Mobility RFS7000 from the network
<MAC>	Identifies the device to remove by its MAC address • <MAC> – Specify the device's MAC address in the AA-BB-CC-DD-EE-FF format.

```
no client-identity <CLIENT-IDENTITY-NAME>
```

no client-identity <CLIENT-IDENTITY-NAME>	Removes the set of client identity fingerprints identified by the <CLIENT-NAME> keyword • <CLIENT-IDENTITY-NAME> – Specify the client identity name.

```
no client-identity-group <CLIENT-IDENTITY-GROUP-NAME>
```

no client-identity-group <CLIENT-IDENTITY-GROUP-NAME>	Removes the client identity group identified by the <CLIENT-IDENTITY-GROUP-NAME> keyword • <CLIENT-IDENTITY-GROUP-NAME> – Specify the client identity group name.

```
no device {containing <WORD>} {(filter type [br650|br6511|
br1220|br71xx|br81xx|rfs4000|rfs6000|rfs7000])}
```

no device	Removes single or multiple devices based on the filter options provided

containing <WORD>	Optional. Removes devices with hostname containing the substring specified by the <WORD> keyword
filter type <DEVICE-TYPE>	Optional. Filters devices based on the device type selected • type <DEVICE-TYPE> – Select the access point or wireless controller type.

```
no customize
[hostname-column-width|show-wireless-client|show-wireless-client-stats|
show-wireless-client-stats-rf|show-wireless-meshpoint|show-wireless-meshpoint
-neighbor-stats|show-wireless-meshpoint-neighbor-stats-rf|show-wireless-radio
|show-wireless-radio-stats|show-wireless-radio-stats-rf]
```

no customize	Restores the output of the show wireless client parameters to default

```
no passowrd-encryption secret 2 <OLD-PASSPHRASE>
```

no password-encryption	Disables password encryption

```
no profile {br650|br6511|br1220|br71xx|br81xx|
|containing|filter} <PROFILE-NAME>
```

no profile	Removes a profile and its associated configurations
br650	Optional. Removes a Brocade Mobility 650 Access Point profile
br6511	Optional. Removes a Brocade Mobility 6511 Access Point profile
br1220	Optional. Removes a Brocade Mobility 1220 Access Point profile
br71xx	Optional. Removes a Brocade Mobility 71XX Access Point profile
rfs4000	Optional. Removes a Brocade Mobility RFS4000 profile
rfs6000	Optional. Removes a Brocade Mobility RFS6000 profile
rfs7000	Optional. Removes a Brocade Mobility RFS7000 profile
<PROFILE-NAME>	Specifies the profile name

```
no wlan [<WLAN-NAME>|all|containing <WLAN-NAME-SUBSTRING>]
```

no wlan	Removes a WLAN
<WLAN-NAME>	Identifies the WLAN name
all	Removes all WLANs
containing <WLAN-NAME-SUBSTRING>	Removes WLANs whose names contain the string specified by the <WLAN-NAME-SUBSTRING> parameter

```
no service set [command-history|reboot-history|upgrade-history] {on
<DEVICE-NAME>}
```

no service set	Resets service command parameters
command-history	Resets command history file size to default (200)
reboot-history	Resets reboot history file size to default (50)
upgrade-history	Resets upgrade history file size to default (50)
on <DEVICE-NAME>	Optional. Resets service command parameters on a specified device • <DEVICE-NAME> – Specify name of the AP, wireless controller, or service platform.

Example

```
rfs7000-37FABE(config)#no ?
  aaa-policy                  Delete a aaa policy
  aaa-tacacs-policy           Delete a aaa tacacs policy
```

```
  advanced-wips-policy        Delete an advanced-wips policy
  alias                       Alias
br650                        Delete an Brocade Mobility 650 Access Point access
point
  br6511                      Delete an Brocade Mobility 6511 Access Point
access point
br1220                      Delete an Brocade Mobility 1220 Access Point access
point
br71xx                      Delete an Brocade Mobility 71XX Access Point access
point
  br81xx                      Delete an Brocade Mobility 1240 Access Point
access point
  ap82xx                      Delete an AP82XX access point
  association-acl-policy      Delete an association-acl policy
  auto-provisioning-policy    Delete an auto-provisioning policy
  captive-portal              Delete a captive portal
  client-identity             Client identity (DHCP Device Fingerprinting)
  client-identity-group       Client identity group (DHCP Fingerprint
                              Database)
  customize                   Restore the custom cli commands to default
  device                      Delete multiple devices
  device-categorization       Delete  device categorization object
  dhcp-server-policy          DHCP server policy
  dns-whitelist               Delete a whitelist object
  event-system-policy         Delete a event system policy
  firewall-policy             Configure firewall policy
  global-association-list     Delete a global association list
  igmp-snoop-policy           Remove device onboard igmp snoop policy
  inline-password-encryption  Disable storing encryption key in the startup
                              configuration file
  ip                          Internet Protocol (IP)
  l2tpv3                      Negate a command or set its defaults
  mac                         MAC configuration
  management-policy           Delete a management policy
  meshpoint                   Delete a meshpoint object
  meshpoint-qos-policy        Delete a mesh point QoS configuration policy
  nac-list                    Delete an network access control list
  passpoint-policy            Delete a passpoint configuration policy
  password-encryption         Disable password encryption in configuration
  profile                     Delete a profile and all its associated
                              configuration
  radio-qos-policy            Delete a radio QoS configuration policy
  radius-group                Local radius server group configuration
  radius-server-policy        Remove device onboard radius policy
  radius-user-pool-policy     Configure Radius User Pool
  rf-domain                   Delete one or more RF-domains and all their
                              associated configurations
  rfs4000                     Delete an Brocade Mobility RFS4000 wireless
controller
  rfs6000                     Delete an Brocade Mobility RFS6000 wireless
controller
  rfs7000                     Delete an Brocade Mobility RFS7000 wireless
controller
  role-policy                 Role based firewall policy
  routing-policy              Policy Based Routing Configuration
  smart-rf-policy             Delete a smart-rf-policy
  wips-policy                 Delete a wips policy
  wlan                        Delete a wlan object
  wlan-qos-policy             Delete a wireless lan QoS configuration policy
```

```
  service                     Service Commands

rfs7000-37FABE(config)#

nx4500-5CFA2B(config)#no ?
  aaa-policy                  Delete a aaa policy
  aaa-tacacs-policy           Delete a aaa tacacs policy
  advanced-wips-policy        Delete an advanced-wips policy
  alias                       Alias
  br650                      Delete an Brocade Mobility 650 Access Point access
  point
  br6511                      Delete an Brocade Mobility 6511 Access Point
  access point
  br1220                      Delete an Brocade Mobility 1220 Access Point
  access point
  br71xx                      Delete an Brocade Mobility 71XX Access Point
  access point
  br81xx                      Delete an Brocade Mobility 1240 Access Point
  access point
  association-acl-policy      Delete an association-acl policy
  auto-provisioning-policy    Delete an auto-provisioning policy
  captive-portal              Delete a captive portal
  client-identity             Client identity (DHCP Device Fingerprinting)
  client-identity-group       Client identity group (DHCP Fingerprint
                              Database)
  customize                   Restore the custom cli commands to default
  device                      Delete multiple devices
  device-categorization       Delete  device categorization object
  dhcp-server-policy          DHCP server policy
  dns-whitelist               Delete a whitelist object
  event-system-policy         Delete a event system policy
  firewall-policy             Configure firewall policy
  igmp-snoop-policy           Remove device onboard igmp snoop policy
  inline-password-encryption  Disable storing encryption key in the startup
                              configuration file
  ip                          Internet Protocol (IP)
  l2tpv3                      Negate a command or set its defaults
  mac                         MAC configuration
  management-policy           Delete a management policy
  meshpoint                   Delete a meshpoint object
  meshpoint-qos-policy        Delete a mesh point QoS configuration policy
  nac-list                    Delete an network access control list
passpoint-policy             Delete a passpoint configuration policy
  password-encryption         Disable password encryption in configuration
  profile                     Delete a profile and all its associated
                              configuration
  radio-qos-policy            Delete a radio QoS configuration policy
  radius-group                Local radius server group configuration
  radius-server-policy        Remove device onboard radius policy
  radius-user-pool-policy     Configure Radius User Pool
  rf-domain                   Delete one or more RF-domains and all their
                              associated configurations
  rfs4000                     Delete an Brocade Mobility RFS4000 wireless
controller
  rfs6000                     Delete an Brocade Mobility RFS6000 wireless
controller
  rfs7000                     Delete an Brocade Mobility RFS7000 wireless
controller
  role-policy                 Role based firewall policy
  routing-policy              Policy Based Routing Configuratino
```

```
  smart-cache-policy          Delete a content caching
  smart-rf-policy             Delete a smart-rf-policy
  url-list                    Delete a URL list
  wips-policy                 Delete a wips policy
  wlan                        Delete a wlan object
  wlan-qos-policy             Delete a wireless lan QoS configuration policy

  service                     Service Commands

nx4500-5CFA2B(config)#
```

passpoint-policy

Global Configuration Commands

Creates a new passpoint policy and enters its configuration mode

The passpoint policy implements the Hotspot 2.0 Wi-Fi Alliance standard, enabling interoperability between clients, infrastructure, and operators. It makes a portion of the IEEE 802.11u standard mandatory and adds Hotspot 2.0 extensions that allow clients to query a network before actually attempting to join it.

The passpoint policy allows a single or set of Hotspot 2.0 configurations to be global and referenced by the devices that use it. It is mapped to a WLAN. However, only primary WLANs on a BSSID will have their passpoint policy configuration used.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
passpoint-policy <POLICY-NAME>
```

Parameters

```
passpoint-policy <POLICY-NAME>
```

passpoint-policy <POLICY-NAME>	Specify the passpoint policy name. If a passpoint policy does not exist, it is created.

Example

```
rfs4000-229D58(config)#passpoint-policy test
rfs4000-229D58(config-passpoint-policy-test)#?

rfs4000-229D58(config-passpoint-policy-test)#?
Passpoint Policy Mode commands:
  3gpp                  Configure a 3gpp plmn (public land mobile network) id
  access-network-type   Set the access network type for the hotspot
  connection-capability Configure the connection capability for the hotspot
  domain-name           Add a domain-name for the hotspot
  hessid                Set a homogeneous ESSID value for the hotspot
  internet              Advertise the hotspot having internet access
```

```
  ip-address-type        Configure the advertised ip-address-type
  nai-realm              Configure a NAI realm for the hotspot
  net-auth-type          Add a network authentication type to the hotspot
  no                     Negate a command or set its defaults
  operator               Add configuration related to the operator of the
                         hotspot
  roam-consortium        Add a roam consortium for the hotspot
  venue                  Set the venue parameters of the hotspot
  wan-metrics            Set the wan-metrics of the hotspot

  clrscr                 Clears the display screen
  commit                 Commit all changes made in this session
  do                     Run commands from Exec mode
  end                    End current mode and change to EXEC mode
  exit                   End current mode and down to previous mode
--More--
rfs4000-229D58(config-passpoint-policy-test)#
```

Related Commands:

no	Removes an existing passpoint policy

NOTE
For more information on passpoint policy, see *Chapter 28, PASSPOINT POLICY*.

password-encryption

Global Configuration Commands

Enables password encryption

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
password-encryption secret 2 <LINE>
```

Parameters

```
password-encryption secret 2 <LINE>
```

secret 2 <LINE>	Encrypts passwords with a secret phrase • 2 – Specifies the encryption type as either SHA256 or AES256 • <LINE> – Specify the encryption passphrase.

Example

```
rfs7000-37FABE(config)#password-encryption secret 2
rfs7000-37FABE(config)#
```

```
nx6500-31FABE(config)#password-encryption secret 2 symbol
nx6500-31FABE(config)#
```

Related Commands:

no	Disables password encryption

profile

Global Configuration Commands

Configures profile related commands. If no parameters are given, all profiles are selected.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
profile {br650|br6511|br1220|br71xx|br81xx|
          containing|filter|rfs4000|rfs6000|rfs7000}

profile {br650|br6511|br1220|br71xx|br81xx|
          rfs4000|rfs6000|rfs7000} <DEVICE-PROFILE-NAME>

profile {containing <DEVICE-PROFILE-NAME>} {filter type [br650|br6511|
          br1220|br71xx|br81xx|rfs4000|rfs6000|rfs7000]}

profile {filter type [br650|br6511|br1220|br71xx|
          br81xx|rfs4000|rfs6000|rfs7000]}
```

Parameters

```
profile {br650|br6511|br1220|br71xx|br81xx|
containing|filter|rfs4000|rfs6000|rfs7000} <DEVICE-PROFILE-NAME>
```

profile	Configures device profile commands. If no device profile is specified, the system configures all device profiles.
br650	Optional. Configures Brocade Mobility 650 Access Point profile commands
br6511	Optional. Configures Brocade Mobility 6511 Access Point profile commands
br1220	Optional. Configures Brocade Mobility 1220 Access Point profile commands
br71xx	Optional. Configures Brocade Mobility 71XX Access Point profile commands
br81xx	Optional. Configures Brocade Mobility 1240 Access Point profile commands
rfs4000	Optional. Configures Brocade Mobility RFS4000 profile commands
rfs6000	Optional. Configures Brocade Mobility RFS6000 profile commands
rfs7000	Optional. Configures Brocade Mobility RFS7000 profile commands
<DEVICE-PROFILE-NAME>	After specifying the profile type, specify a substring in the profile name to filter profiles

```
profile {containing <DEVICE-PROFILE-NAME>} {filter type [br650|br6511|
br1220|br71xx|br81xx|rfs4000|rfs6000|rfs7000]}
```

profile	Configures device profile commands
containing <DEVICE-PROFILE-NAME>	Optional. Configures profiles that contain a specified sub-string in the hostname • <DEVICE-PROFILE-NAME> – Specify a substring in the profile name to filter profiles.
filter type	Optional. An additional filter used to configure a specific type of device profile. If no device type is specified, the system configures all device profiles. • type – Filters profiles by the device type. Select a device type from the following options:
br650	Optional. Selects an Brocade Mobility 650 Access Point profile
br6511	Optional. Selects an Brocade Mobility 6511 Access Point profile
br1220	Optional. Selects an Brocade Mobility 1220 Access Point profile
br71xx	Optional. Selects an Brocade Mobility 71XX Access Point profile
br81xx	Optional. Selects an Brocade Mobility 1240 Access Point profile
rfs4000	Optional. Selects a Brocade Mobility RFS4000 profile
rfs6000	Optional. Selects a Brocade Mobility RFS6000 profile
rfs7000	Optional. Selects a Brocade Mobility RFS7000 profile

```
profile {filter type [br650|br6511|br1220|br71xx|
br81xx|rfs4000|rfs6000|rfs7000]}
```

profile	Configures device profile commands
filter type	Optional. An additional filter used to configure a specific type of device profile. If no device type is specified, the system configures all device profiles. • type – Filters profiles by the device type. Select a device type from the following options:
br650	Optional. Selects an Brocade Mobility 650 Access Point profile
br6511	Optional. Selects an Brocade Mobility 6511 Access Point profile
br1220	Optional. Selects an Brocade Mobility 1220 Access Point profile
br71xx	Optional. Selects an Brocade Mobility 71XX Access Point profile
br81xx	Optional. Selects an Brocade Mobility 1240 Access Point profile
rfs4000	Optional. Selects a Brocade Mobility RFS4000 profile
rfs6000	Optional. Selects a Brocade Mobility RFS6000 profile
rfs7000	Optional. Selects a Brocade Mobility RFS7000 profile

Example

```
rfs7000-37FABE(config)#profile rfs7000 default-rfs7000
rfs7000-37FABE(config-profile-default-rfs7000)#?
Profile Mode commands:
  adopter-auto-provisioning-policy-lookup  Use centralized auto-provisioning
                                           policy when adopted by another
                                           controller
  alias                                    Alias
  area                                    Set name of area where the system
                                           is located
  arp                                      Address Resolution Protocol (ARP)
  auto-learn-staging-config                Enable learning network
                                           configuration of the devices that
                                           come for adoption
```

autogen-uniqueid	Autogenerate a unique id
autoinstall	Autoinstall settings
bridge	Ethernet bridge
captive-portal	Captive portal
cdp	Cisco Discovery Protocol
cluster	Cluster configuration
configuration-persistence	Enable persistence of configuration across reloads (startup config file)
controller	WLAN controller configuration
critical-resource	Critical Resource
crypto	Encryption related commands
device-upgrade	Device firmware upgrade
dot1x	802.1X
dscp-mapping	Configure IP DSCP to 802.1p priority mapping for untagged frames
email-notification	Email notification configuration
enforce-version	Check the firmware versions of devices before interoperating
environmental-sensor	Environmental Sensors Configuration
events	System event messages
export	Export a file
floor	Set the floor within a area where the system is located
gre	GRE protocol
http-analyze	Specify HTTP-Analysis configuration
interface	Select an interface to configure
ip	Internet Protocol (IP)
l2tpv3	L2tpv3 protocol
l3e-lite-table	L3e lite Table
led	Turn LEDs on/off on the device
legacy-auto-downgrade	Enable device firmware to auto downgrade when other legacy devices are detected
legacy-auto-update	Auto upgrade of legacy devices
lldp	Link Layer Discovery Protocol
load-balancing	Configure load balancing parameter
logging	Modify message logging facilities
mac-address-table	MAC Address Table
mac-auth	802.1X
memory-profile	Memory profile to be used on the device
meshpoint-device	Configure meshpoint device parameters
meshpoint-monitor-interval	Configure meshpoint monitoring
min-misconfiguration-recovery-time	Check controller connectivity after configuration is received
mint	MiNT protocol
misconfiguration-recovery-time	Check controller connectivity after configuration is received
neighbor-inactivity-timeout	Configure neighbor inactivity timeout
neighbor-info-interval	Configure neighbor information exchange interval
no	Negate a command or set its defaults
noc	Configure the noc related setting
ntp	Ntp server A.B.C.D
power-config	Configure power mode

```
  preferred-controller-group              Controller group this system will
                                          prefer for adoption
  preferred-tunnel-controller             Tunnel Controller Name this system
                                          will prefer for tunneling extended
                                          vlan traffic
  radius                                  Configure device-level radius
                                          authentication parameters
  rf-domain-manager                       RF Domain Manager
  router                                  Dynamic routing
  spanning-tree                           Spanning tree
  tunnel-controller                       Tunnel Controller group this
                                          controller belongs to
  use                                     Set setting to use
  vrrp                                    VRRP configuration
  wep-shared-key-auth                     Enable support for 802.11 WEP
                                          shared key authentication

  clrscr                                  Clears the display screen
  commit                                  Commit all changes made in this
                                          session
  do                                      Run commands from Exec mode
  end                                     End current mode and change to EXEC
                                          mode
  exit                                    End current mode and down to
                                          previous mode
  help                                    Description of the interactive help
                                          system
  revert                                  Revert changes
  service                                 Service Commands
  show                                    Show running system information
  write                                   Write running configuration to
                                          memory or terminal

rfs4000-229D58(config-profile-de)#

rfs7000-37FABE(config-profile-default-rfs7000)#

nx4500-5CFA2B(config-profile-test)#?
Profile Mode commands:
  adopter-auto-provisioning-policy-lookup  Use centralized auto-provisioning
                                           policy when adopted by another
                                           controller
  alias                                    Alias
  area                                     Set name of area where the system
                                           is located
  arp                                      Address Resolution Protocol (ARP)
  auto-learn-staging-config                Enable learning network
                                           configuration of the devices that
                                           come for adoption
  autogen-uniqueid                         Autogenerate a unique id
  autoinstall                              Autoinstall settings
  bridge                                   Ethernet bridge
  captive-portal                           Captive portal
  cdp                                      Cisco Discovery Protocol
  cluster                                  Cluster configuration
  configuration-persistence                Enable persistence of configuration
                                           across reloads (startup config
                                           file)
  controller                               WLAN controller configuration
  critical-resource                        Critical Resource
```

crypto	Encryption related commands
device-upgrade	Device firmware upgrade
dot1x	802.1X
dscp-mapping	Configure IP DSCP to 802.1p priority mapping for untagged frames
email-notification	Email notification configuration
enforce-version	Check the firmware versions of devices before interoperating
environmental-sensor	Environmental Sensors Configuration
events	System event messages
export	Export a file
floor	Set the floor within a area where the system is located
gre	GRE protocol
http-analyze	Specify HTTP-Analysis configuration
interface	Select an interface to configure
ip	Internet Protocol (IP)
l2tpv3	L2tpv3 protocol
l3e-lite-table	L3e lite Table
led	Turn LEDs on/off on the device
legacy-auto-downgrade	Enable device firmware to auto downgrade when other legacy devices are detected
legacy-auto-update	Auto upgrade of legacy devices
lldp	Link Layer Discovery Protocol
load-balancing	Configure load balancing parameter
logging	Modify message logging facilities
mac-address-table	MAC Address Table
mac-auth	802.1X
memory-profile	Memory profile to be used on the device
meshpoint-device	Configure meshpoint device parameters
meshpoint-monitor-interval	Configure meshpoint monitoring interval
min-misconfiguration-recovery-time	Check controller connectivity after configuration is received
mint	MiNT protocol
misconfiguration-recovery-time	Check controller connectivity after configuration is received
neighbor-inactivity-timeout	Configure neighbor inactivity timeout
neighbor-info-interval	Configure neighbor information exchange interval
no	Negate a command or set its defaults
noc	Configure the noc related setting
ntp	Ntp server A.B.C.D
power-config	Configure power mode
preferred-controller-group	Controller group this system will prefer for adoption
preferred-tunnel-controller	Tunnel Controller Name this system will prefer for tunneling extended vlan traffic
radius	Configure device-level radius authentication parameters
rf-domain-manager	RF Domain Manager
router	Dynamic routing
slot	PCI expansion slot

```
spanning-tree                  Spanning tree
tunnel-controller              Tunnel Controller group this
                               controller belongs to
use                            Set setting to use
vrrp                           VRRP configuration
wep-shared-key-auth            Enable support for 802.11 WEP
                               shared key authentication

clrscr                         Clears the display screen
commit                         Commit all changes made in this
                               session
do                             Run commands from Exec mode
end                            End current mode and change to EXEC
                               mode
exit                           End current mode and down to
                               previous mode
help                           Description of the interactive help
                               system
revert                         Revert changes
service                        Service Commands
show                           Show running system information
write                          Write running configuration to
                               memory or terminal

nx4500-5CFA2B(config-profile-test)#
```

NOTE
For more information on profiles and how to configure profiles, see *Chapter 7, PROFILES*.

Related Commands:

no	Removes a profile and its associated configurations

radio-qos-policy

Global Configuration Commands

Configures a radio *quality-of-service* (QoS) policy

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
radio-qos-policy <RADIO-QOS-POLICY-NAME>
```

Parameters

```
radio-qos-policy <RADIO-QOS-POLICY-NAME>
```

<RADIO-QOS-POLICY-NAME>	Specify the radio QoS policy name. If the policy does not exist, it is created.

Example

```
rfs7000-37FABE(config)#radio-qos-policy test
rfs7000-37FABE(config-radio-qos-test)#?
Radio QoS Mode commands:
  accelerated-multicast  Configure multicast streams for acceleration
  admission-control      Configure admission-control on this radio for one or
                         more access categories
  no                     Negate a command or set its defaults
  smart-aggregation      Configure smart aggregation parameters
  wmm                    Configure 802.11e/Wireless MultiMedia parameters

  clrscr                 Clears the display screen
  commit                 Commit all changes made in this session
  do                     Run commands from Exec mode
  end                    End current mode and change to EXEC mode
  exit                   End current mode and down to previous mode
  help                   Description of the interactive help system
  revert                 Revert changes
  service                Service Commands
  show                   Show running system information
  write                  Write running configuration to memory or terminal

rfs7000-37FABE(config-radio-qos-test)#
```

NOTE
For more information on radio qos policy, see *Chapter 18, RADIO-QOS-POLICY*.

Related Commands:

no	Removes an existing Radio QoS policy

radius-group

Global Configuration Commands

Configures RADIUS user group parameters

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
radius-group <RADIUS-GROUP-NAME>
```

Parameters

```
radius-group <RADIUS-GROUP-NAME>
```

<RADIUS-GROUP-NAME>	Specify a RADIUS user group name. The name should not exceed 64 characters. If the RADIUS user group does not exist, it is created.

Example

```
rfs7000-37FABE(config)#radius-group testgroup
rfs7000-37FABE(config-radius-group-testgroup)#?
Radius user group configuration commands:
  guest       Make this group a Guest group
  no          Negate a command or set its defaults
  policy      Radius group access policy configuration
  rate-limit  Set rate limit for group

  clrscr      Clears the display screen
  commit      Commit all changes made in this session
  do          Run commands from Exec mode
  end         End current mode and change to EXEC mode
  exit        End current mode and down to previous mode
  help        Description of the interactive help system
  revert      Revert changes
  service     Service Commands
  show        Show running system information
  write       Write running configuration to memory or terminal

rfs7000-37FABE(config-radius-group-testgroup)#
```

NOTE
For more information on RADIUS user group commands, see *Chapter 17, RADIUS-POLICY*.

Related Commands:

no	Removes an existing RADIUS group

radius-server-policy

Global Configuration Commands

Creates an onboard device RADIUS policy

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
radius-server-policy <RADIUS-SERVER-POLICY-NAME>
```

Parameters

```
radius-server-policy <RADIUS-SERVER-POLICY-NAME>
```

<RADIUS-SERVER-POLICY-NAME>	Specify the RADIUS server policy name. If the policy does not exist, it is created.

Example

```
rfs7000-37FABE(config)#radius-server-policy testpolicy
rfs7000-37FABE(config-radius-server-policy-testpolicy)#?
Radius Configuration commands:
  authentication           Radius authentication
  chase-referral           Enable chasing referrals from LDAP server
  crl-check                Enable Certificate Revocation List( CRL ) check
  ldap-group-verification  Enable LDAP Group Verification setting
  ldap-server              LDAP server parameters
  local                    RADIUS local realm
  nas                      RADIUS client
  no                       Negate a command or set its defaults
  proxy                    RADIUS proxy server
  session-resumption       Enable session resumption/fast reauthentication by
                           using cached attributes
  use                      Set setting to use

  clrscr                   Clears the display screen
  commit                   Commit all changes made in this session
  do                       Run commands from Exec mode
  end                      End current mode and change to EXEC mode
  exit                     End current mode and down to previous mode
  help                     Description of the interactive help system
  revert                   Revert changes
  service                  Service Commands
  show                     Show running system information
  write                    Write running configuration to memory or terminal

rfs7000-37FABE(config-radius-server-policy-testpolicy)#
```

NOTE
For more information on RADIUS server policy commands, see *Chapter 17, RADIUS-POLICY*.

Related Commands:

no	Removes an existing RADIUS server policy

radius-user-pool-policy

Global Configuration Commands

Configures a RADIUS user pool

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
radius-user-pool-policy <RADIUS-USER-POOL-POLICY-NAME>
```

Parameters

```
radius-user-pool-policy <RADIUS-USER-POOL-POLICY-NAME>
```

<RADIUS-USER-POOL-POLICY-NAME>	Specify the RADIUS user pool policy name. If the policy does not exist, it is created.

Example

```
rfs7000-37FABE(config)#radius-user-pool-policy testpool
rfs7000-37FABE(config-radius-user-pool-testpool)#?
Radius User Pool Mode commands:
  no       Negate a command or set its defaults
  user     Radius user configuration

  clrscr   Clears the display screen
  commit   Commit all changes made in this session
  do       Run commands from Exec mode
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  revert   Revert changes
  service  Service Commands
  show     Show running system information
  write    Write running configuration to memory or terminal

rfs7000-37FABE(config-radius-user-pool-testpool)#
```

NOTE
For more information on RADIUS user group commands, see *Chapter 17, RADIUS-POLICY*.

Related Commands:

no	Removes an existing RADIUS user pool

rename

Global Configuration Commands

Renames and existing TLO

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
rename tlo <TLO-NAME>
```

Parameters

```
rename tlo <TLO-NAME> <NEW-TLO-NAME>
```

rename tlo <TLO-NAME> <NEW-TLO-NAME>	Renames an existing TLO object • <TLO-NAME> – Specify the TLO's name. This is the TLO that is to be renamed. • <NEW-TLO-NAME> – Specify the new name for this TLO Enter rename and press **Tab** to list top level objects available for renaming.

Example

The following example shows the top level objects available for renaming:

```
rfs4000-229D58(config)#rename
aaa_policy                aaa_tacacs_policy         address_range_alias
assoc_acl                 auto_provisioning_policy  bridging_policy
captive_portal            centro_policy             client_identity
client_identity_group     device_categorization     dhcp_server_policy
dns_whitelist             event_system_policy       firewall_policy
global_assoc_list         host_alias                ip_acl
l2tpv3_policy             mac_acl                   management_policy
meshpoint                 meshpoint_qos             mint_policy
mint_security_policy      nac_list                  network_alias
passpoint_policy          profile                   radio_qos
radius_group              radius_server_policy      radius_user_pool
rf_domain                 rls_policy                role_policy
routing_policy            runtime_license           service_alias
smart_rf_policy           subscriber_policy         vlan_alias
wips_policy               wlan                      wlan_qos
wsm_policy                device
rfs4000-229D58(config)#
```

The following examples first clones the existing IP access list **BROADCAST-MULTICAST-CONTROL**, and then renames the cloned IP access list:

```
rfs4000-229D58(config)#show context
!
! Configuration of Brocade Mobility RFS4000 version 5.5.0.0-018D
!
!
version 2.1
!
!
client-identity TestClientIdentity
 dhcp 1 message-type request option-codes exact hexstring 5e4d36780b3a7f
!
client-identity-group ClientIdentityGroup
 client-identity TestClientIdentity precedence 1
!
ip access-list BROADCAST-MULTICAST-CONTROL
 permit tcp any any rule-precedence 10 rule-description "permit all TCP
traffic"
 permit udp any eq 67 any eq dhcpc rule-precedence 11 rule-description "permit
DHCP replies"
 deny udp any range 137 138 any range 137 138 rule-precedence 20
rule-description "deny windows netbios"
 deny ip any 224.0.0.0/4 rule-precedence 21 rule-description "deny IP
multicast"
 deny ip any host 255.255.255.255 rule-precedence 22 rule-description "deny IP
local broadcast"
```

```
 permit ip any any rule-precedence 100 rule-description "permit all IP
traffic"
!
mac access-list PERMIT-ARP-AND-IPv4
 permit any any type ip rule-precedence 10 rule-description "permit all IPv4
traffic"
--More--
rfs4000-229D58(config)

rfs4000-229D58(config)#clone ip_acl BROADCAST-MULTICAST-CONTROL TestIP_CLONED
rfs4000-229D58(config)#commit

rfs4000-229D58(config)#show context
!
! Configuration of Brocade Mobility RFS4000 version 5.5.0.0-018D
!
!
version 2.1
!
!
client-identity TestClientIdentity
 dhcp 1 message-type request option-codes exact hexstring 5e4d36780b3a7f
!
client-identity-group ClientIdentityGroup
 client-identity TestClientIdentity precedence 1
!
ip access-list BROADCAST-MULTICAST-CONTROL
 permit tcp any any rule-precedence 10 rule-description "permit all TCP
traffic"
 permit udp any eq 67 any eq dhcpc rule-precedence 11 rule-description "permit
DHCP replies"
 deny udp any range 137 138 any range 137 138 rule-precedence 20
rule-description "deny windows netbios"
 deny ip any 224.0.0.0/4 rule-precedence 21 rule-description "deny IP
multicast"
 deny ip any host 255.255.255.255 rule-precedence 22 rule-description "deny IP
local broadcast"
 permit ip any any rule-precedence 100 rule-description "permit all IP
traffic"
!
ip access-list TestIP_CLONED
 permit tcp any any rule-precedence 10 rule-description "permit all TCP
traffic"
 permit udp any eq 67 any eq dhcpc rule-precedence 11 rule-description "permit
DHCP replies"
--More--
rfs4000-229D58(config)#

rfs4000-229D58(config)#rename ip_acl TestIP_CLONED TestIP_RENAMED
rfs4000-229D58(config)#commit

rfs4000-229D58(config)#show context
!
! Configuration of Brocade Mobility RFS4000 version 5.5.0.0-018D
!
!
version 2.1
!
!
client-identity TestClientIdentity
```

```
 dhcp 1 message-type request option-codes exact hexstring 5e4d36780b3a7f
!
client-identity-group ClientIdentityGroup
 client-identity TestClientIdentity precedence 1
!
ip access-list BROADCAST-MULTICAST-CONTROL
 permit tcp any any rule-precedence 10 rule-description "permit all TCP
traffic"
 permit udp any eq 67 any eq dhcpc rule-precedence 11 rule-description "permit
DHCP replies"
 deny udp any range 137 138 any range 137 138 rule-precedence 20
rule-description "deny windows netbios"
 deny ip any 224.0.0.0/4 rule-precedence 21 rule-description "deny IP
multicast"
 deny ip any host 255.255.255.255 rule-precedence 22 rule-description "deny IP
local broadcast"
 permit ip any any rule-precedence 100 rule-description "permit all IP
traffic"
!
ip access-list TestIP_RENAMED
 permit tcp any any rule-precedence 10 rule-description "permit all TCP
traffic"
 permit udp any eq 67 any eq dhcpc rule-precedence 11 rule-description "permit
DHCP replies"
--More--
rfs4000-229D58(config)#
```

Related Commands:

clone	Creates a replica of an existing TLO or device

rf-domain

Global Configuration Commands

An RF Domain groups devices that can logically belong to one network.

The following table lists the RF Domain configuration mode commands.

Command	Description	Reference
rf-domain	Creates a RF Domain policy and enters its configuration mode	page 284
rf-domain-mode commands	Invokes RF Domain configuration mode commands	page 286

rf-domain

rf-domain

Creates an RF Domain or enters the RF Domain configuration context for one or more RF Domains. If the RF Domain does not exist, it is created.

The configuration of controllers (wireless controllers, service platforms, and access points) comprises of RF Domains that define regulatory, location, and other relevant policies. At least one default RF Domain is assigned to each controller.

RF Domains allow administrators to assign configuration data to multiple devices deployed in a common coverage area, such as in a floor, building, or site. Each RF Domain contains policies that set the Smart RF or WIPS configuration.

RF Domains also enable administrators to override WLAN SSID name and VLAN assignments. This enables the deployment of a global WLAN across multiple sites and unique SSID name or VLAN assignments to groups of access points servicing the global WLAN. This WLAN override eliminates the need to define and manage a large number of individual WLANs and profiles.

A controller's configuration contains:

- A default RF Domain - Each controller utilizes a default RF Domain. Access Points are assigned to this default RF Domain as they are discovered by the controller. A default RF Domain can be used for single-site and multi-site deployments.
  - Single-site deployment – The default RF Domain can be used for single site deployments, where regional, regulatory, and RF policies are common between devices.
  - Multi-site deployment – A default RF Domain can omit configuration parameters to prohibit regulatory configuration from automatically being inherited by devices as they are discovered. This is desirable in multi-site deployments with devices spanning multiple countries. Omitting specific configuration parameters eliminates the risk of an incorrect country code from being automatically assigned to a device.
- A user-defined RF Domain - Created by administrators. A user-defined RF Domain can be assigned to multiple devices manually or automatically.
  - Manually assigned – Use the CLI or UI to manually assign a user-defined RF Domain to controllers and service platforms.
  - Automatically assigned – Use a AP provisioning policy to automatically assign specific RF Domains to access points based on the access point's model, serial number, VLAN, DHCP option, and IP address or MAC address. Automatic RF Domain assignments are useful in large deployments, as they enable plug-n-play access point deployments by automatically applying RF Domains to remote access points. For more information on auto provisioning policy, see *AUTO-PROVISIONING-POLICY*.

    Configure and deploy user-defined RF Domains for single or multiple sites where devices require unique regulatory and regional configurations, or unique Smart RF and WIPS policies. User-defined RF Domains can be used to:
  - Assign unique Smart RF or WIPS policies to access points deployed on different floors or buildings within in a site.
  - Assign unique regional or regulatory configurations to devices deployed in different states or countries.
  - Assign unique WLAN SSIDs and/or VLAN IDs to sites assigned a common WLAN without having to define individual WLANs for each site.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
rf-domain {<RF-DOMAIN-NAME>|containing <DOMAIN-NAME>}
```

Parameters

```
rf-domain {<RF-DOMAIN-NAME>|containing <DOMAIN-NAME>}
```

rf-domain	Creates a new RF Domain or enters its configuration context
<RF-DOMAIN-NAME>	Optional. Specify the RF Domain name (should not exceed 32 characters and should represent the intended purpose). Once created, the name cannot be edited.
containing <DOMAIN-NAME>	Optional. Identifies an existing RF Domain that contains a specified sub-string in the domain name • <DOMAIN-NAME> – Specify a sub-string of the RF Domain name.

Example

```
rfs7000-37FABE(config)#rf-domain rfs7000
rfs7000-37FABE(config-rf-domain-rfs7000)#?
RF Domain Mode commands:
  alias               Alias
  channel-list        Configure channel list to be advertised to wireless
                      clients
  contact             Configure the contact
  control-vlan        VLAN for control traffic on this RF Domain
  controller-managed  RF Domain manager for this domain will be an adopting
                      controller
  country-code        Configure the country of operation
  layout              Configure layout
  location            Configure the location
  mac-name            Configure MAC address to name mappings
  no                  Negate a command or set its defaults
  override-smartrf    Configured RF Domain level overrides for smart-rf
  override-wlan       Configure RF Domain level overrides for wlan
  sensor-server       Motorola AirDefense sensor server configuration
  stats               Configure the stats related setting
  timezone            Configure the timezone
  tree-node           Configure tree node under which this rf-domain appears
  use                 Set setting to use
  clrscr              Clears the display screen
  commit              Commit all changes made in this session
  do                  Run commands from Exec mode
  end                 End current mode and change to EXEC mode
  exit                End current mode and down to previous mode
  help                Description of the interactive help system
  revert              Revert changes
  service             Service Commands
  show                Show running system information
  write               Write running configuration to memory or terminal
rfs7000-37FABE(config-rf-domain-rfs7000)#
```

rf-domain-mode commands

rf-domain

This section describes the default commands under RF Domain.

The following table summarises RF Domain configuration commands.

Command	Description	Reference
alias	Configures network, VLAN, and service aliases at the RF Domain level	page 287
channel-list	Configures the channel list advertised by radios	page 292
contact	Configures network administrator's contact information (needed in case of any problems impacting the RF Domain)	*page 4-293*
control-vlan	Configures VLAN for traffic control on a RF Domain	page 294
controller-managed	Configures the adopting controller or service platform as this RF Domain's manager	page 295
country-code	Configures the country of operation	*page 4-295*
layout	Configures layout information	page 296
location	Configures the physical location of a RF Domain	page 297
mac-name	Maps MAC addresses to names	*page 4-298*
no	Negates a command or reverts configured settings to their default	*page 4-299*
override-smart-rf	Configures RF Domain level overrides for Smart RF	*page 4-301*
override-wlan	Configures RF Domain level overrides for a WLAN	*page 4-302*
sensor-server	Configures an AirDefense sensor server on this RF Domain	*page 4-303*
stats	Configures stats related settings on this RF Domain. These settings define how RF Domain statistics are updated	*page 4-304*
timezone	Configures a RF Domain's geographic time zone	*page 4-306*
tree-node	Configures the hierarchial (tree-node) structure under which this RF Domain appears	page 306
use	Enables the use of a specified Smart RF and/or WIPS policy	page 308
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

alias

rf-domain-mode commands

Configures network, VLAN, host, string, and network-service aliases at the RF Domain level

This command also allows you to associate existing aliases, created in the global configuration mode, and apply overrides to customize for use at the domain level.

For information on aliases, see *alias*.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
alias [address-range|host|network|network-group|network-service|string|vlan]

alias address-range <ADDRESS-RANGE-ALIAS-NAME> <STARTING-IP> to <ENDING-IP>

alias host <HOST-ALIAS-NAME> <HOST-IP>

alias network <NETWORK-ALIAS-NAME> <NETWORK-ADDRESS/MASK>

alias network-group <NETWORK-GROUP-ALIAS-NAME> [address-range|host|network]
alias network-group <NETWORK-GROUP-ALIAS-NAME> [address-range <STARTING-IP> to
          <ENDING-IP> {<STARTING-IP> to <ENDING-IP>}|host <HOST-IP>
{<HOST-IP>}|
          network <NETWORK-ADDRESS/MASK> {<NETWORK-ADDRESS/MASK>}]

alias network-service <NETWORK-SERVICE-ALIAS-NAME> proto
[<0-254>|<WORD>|eigrp|gre|
          igmp|igp|ospf|vrrp]
{(<1-65535>|<WORD>|bgp|dns|ftp|ftp-data|gopher|https|ldap|nntp|
          ntp|pop3|proto|sip|smtp|sourceport|ssh|telnet|tftp|www)}

alias network-service <NETWORK-SERVICE-ALIAS-NAME> proto
[<0-254>|<WORD>|eigrp|gre|
          igmp|igp|ospf|vrrp]
{(<1-65535>|<WORD>|bgp|dns|ftp|ftp-data|gopher|https|ldap|nntp|
          ntp|pop3|proto|sip|smtp|sourceport
[<1-65535>|<WORD>]|ssh|telnet|tftp|www)}

alias string <STRING-ALIAS-NAME> <LINE>

alias vlan <VLAN-ALIAS-NAME> <1-4094>
```

Parameters

```
alias address-range <ADDRESS-RANGE-ALIAS-NAME> <STARTING-IP> to <ENDING-IP>
```

address-range <ADRESS-RANGE-ALIAS-NAME>	Creates a new address-range alias for this RF Domain. Or associates an existing address-range alias with this RF Domain. An address-range alias maps a name to a range of IP addresses. • <ADRESS-RANGE-ALIAS-NAME> – Specify the address range alias name. Alias name should begin with '$'.
<STARTING-IP> to <ENDING-IP>	Associates a range of IP addresses with this address range alias • <STARTING-IP> – Specify the first IP address in the range. • to <ENDING-IP> – Specify the last IP address in the range. If using an existing address-range alias, you can apply overrides to the alias at the RF Domain level.

	`alias host <HOST-ALIAS-NAME> <HOST-IP>`
host <HOST-ALIAS-NAME>	Creates a host alias for this RF Domain. Or associates an existing host alias with this RF Domain. A host alias maps a name to a single network host. • <HOST-ALIAS-NAME> – Specify the host alias name. Alias name should begin with '$'.
<HOST-IP>	Associates the network host's IP address with this host alias • <HOST-IP> – Specify the network host's IP address. If using an existing host alias, you can apply overrides to the alias at the RF Domain level.

	`alias network <NETWORK-ALIAS-NAME> <NETWORK-ADDRESS/MASK>`
network <NETWORK-ALIAS-NAME>	Creates a network alias for this RF Domain. Or associates an existing network alias with this RF Domain. A network alias maps a name to a single network address. • <NETWORK-ALIAS-NAME> – Specify the network alias name. Alias name should begin with '$'.
<NETWORK-ADDRESS/MASK>	Associates a single network with this network alias • <NETWORK-ADDRESS/MASK> – Specify the network's address and mask. If using an existing network alias, you can apply overrides to the alias at the RF Domain level.

	`alias network-group <NETWORK-GROUP-ALIAS-NAME> [address-range <STARTING-IP> to <ENDING-IP> {<STARTING-IP> to <ENDING-IP>}|host <HOST-IP> {<HOST-IP>}| network <NETWORK-ADDRESS/MASK> {<NETWORK-ADDRESS/MASK>}`
network <NETWORK-GROUP-ALIAS-NAME>	Creates a network-group alias for this RF Domain. Or associates an existing network-group alias with this RF Domain. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name. Alias name should begin with '$'. After specifying the name, specify the following: a range of IP addresses, host addresses, or a range of network addresses. If using an existing network-group alias, you can apply overrides to the alias at the RF Domain level.
address-range <STARTING-IP> to <ENDING-IP> {<STARTING-IP> to <ENDING-IP>}	Associates a range of IP addresses with this network-group alias • <STARTING-IP> – Specify the first IP address in the range. • to <ENDING-IP> – Specify the last IP address in the range. • <STARTING-IP> to <ENDING-IP> – Optional. Specifies more than one range of IP addresses. A maximum of eight (8) IP address ranges can be configured.
host <HOST-IP> {<HOST-IP>}	Associates a single or multiple hosts with this network-group alias • <HOST-IP> – Specify the hosts' IP address. • <HOST-IP> – Optional. Specifies more than one host. A maximum of eight (8) hosts can be configured.
network <NETWORK-ADDRESS/MASK> {<NETWORK-ADDRESS/MASK>}	Associates a single or multiple networks with this network-group alias • <NETWORK-ADDRESS/MASK> – Specify the network's address and mask. • <NETWORK-ADDRESS/MASK> – Optional. Specifies more than one network. A maximum of eight (8) networks can be configured.

```
alias network-service <NETWORK-SERVICE-ALIAS-NAME> proto
[<0-254>|<WORD>|eigrp|gre|
igmp|igp|ospf|vrrp]
{(<1-65535>|<WORD>|bgp|dns|ftp|ftp-data|gopher|https|ldap|nntp|
ntp|pop3|proto|sip|smtp|sourceport [<1-65535>|<WORD>]|ssh|telnet|tftp|www)}
```

alias network-service <NETWORK-SERVICE-ALIAS-NAME>	Creates a network-service alias for this RF Domain. Or associates an existing network-service alias with this RF Domain. A network-service alias maps a name to network services and the corresponding source and destination software ports. • <NETWORK-SERVICE-ALIAS-NAME> – Specify a network-service alias name. Alias name should begin with '$'. If using an existing network-service alias, you can apply overrides to the alias at the RF Domain level.
proto [<0-254>| <WORD>|eigrp|gre| igmp|igp|ospf|vrrp]	Use one of the following options to associate an Internet protocol with this network-service alias: • <0-254> – Identifies the protocol by its number. Specify the protocol number from 0 - 254. This is the number by which the protocol is identified in the *Protocol* field of the IPv4 header and the *Next Header* field of IPv6 header. For example, the *User Datagram Protocol's* (UDP) designated number is 17. • <WORD> – Identifies the protocol by its name. Specify the protocol name. • eigrp – Selects *Enhanced Interior Gateway Routing Protocol* (EIGRP). The protocol number 88. • gre – Selects *Generic Routing Encapsulation* (GRE). The protocol number is 47. • igmp – Selects *Internet Group Management Protocol* (IGMP). The protocol number is 2. • igp – Selects *Interior Gateway Protocol* (IGP). The protocol number is 9. • ospf – Selects *Open Shortest Path First* (OSPF). The protocol number is 89. • vrrp – Selects *Virtual Router Redundancy Protocol* (VRRP). The protocol number is 112.
<1-65535>|<WORD>| bgp|dns|ftp|ftp-data| gopher|https|ldap|nntp| ntp|pop3|proto|sip|smtp| sourceport [<1-65535>| <WORD>]|ssh|telnet| tftp|www)}	After specifying the protocol, you may configure a destination port for this service. These keywords are recursive and you can configure multiple protocols and associate multiple destination and source ports. • <1-65535> – Optional. Configures a destination port number from 1 - 65535 • <WORD> – Optional. Identifies the destination port by the service name provided. For example, the *secure shell* (SSH) service uses TCP port 22. • bgp – Optional. Configures the default *Border Gateway Protocol* (BGP) services port (179) • dns – Optional. Configures the default *Domain Name System* (DNS) services port (53) • ftp – Optional. Configures the default *File Transfer Protocol* (FTP) control services port (21) • ftp-data – Optional. Configures the default FTP data services port (20) • gopher – Optional. Configures the default gopher services port (70) • https – Optional. Configures the default HTTPS services port (443) • ldap – Optional. Configures the default *Lightweight Directory Access Protocol* (LDAP) services port (389) • nntp – Optional. Configures the default Newsgroup (NNTP) services port (119) • ntp – Optional. Configures the default *Network Time Protocol* (NTP) services port (123) • POP3 – Optional. Configures the default *Post Office Protocol* (POP3) services port (110) • proto – Optional. Use this option to select another Internet protocol in addition to the one selected in the previous step. Contd..

	• sip – Optional. Configures the default *Session Initiation Protocol* (SIP) services port (5060)
	• smtp – Optional. Configures the default *Simple Mail Transfer Protocol* (SMTP) services port (25)
	• sourceport [<1-65535>|<WORD>] – Optional. After specifying the destination port, you may specify a single or range of source ports.
	  • <1-65535> – Specify the source port from 1 - 65535.
	  • <WORD> – Specify the source port range, for example 1-10.
	• ssh – Optional. Configures the default SSH services port (22)
	• telnet – Optional. Configures the default Telnet services port (23)
	• tftp – Optional. Configures the default *Trivial File Transfer Protocol* (TFTP) services port (69)
	• www – Optional. Configures the default HTTP services port (80)

`alias string <STRING-ALIAS-NAME> <LINE>`

alias string <STRING-ALIAS-NAME>	Creates a string alias for this RF Domain. Or associates an existing string alias with this RF Domain. String aliases map a name to an arbitrary string value. For example, alias string $DOMAIN test.brocade.com'. In this example, the string alias name is: *$DOMAIN* and the string value it is mapped to is: *test.brocade.com*. In this example, the string alias refers to a domain name. • <VLAN-ALIAS-NAME> – Specify the string alias name. • <LINE> – Specify the string value. Alias name should begin with '$'. If using an existing string alias, you can apply overrides to the alias at the RF Domain level.

`alias vlan <VLAN-ALIAS-NAME> <1-4094>`

alias vlan <VLAN-ALIAS-NAME>	Creates a VLAN alias for this RF Domain. Or associates an existing VLAN alias with this RF Domain. A VLAN alias maps a name to a VLAN ID. • <VLAN-ALIAS-NAME> – Specify the VLAN alias name. Alias name should begin with '$'.
<1-4094>	Maps the VLAN alias to a VLAN ID • <1-4094> – Specify the VLAN ID from 1 - 4094. If using an existing VLAN alias, you can apply overrides to the alias at the RF Domain level.

Example

```
rfs4000-229D58(config)#show context
!
! Configuration of Brocade Mobility RFS4000 version 5.5.0.0-053B
!
!
version 2.3
!
!
alias network-group $TestNetGrpAlias network 192.168.13.0/24 192.168.16.0/24
alias network-group $TestNetGrpAlias address-range 192.168.13.7 to
192.168.13.16 192.168.13.20 to 192.168.13.25
!
alias network $TestNetworkAlias 192.168.13.0/24
!
alias host $TestHostAlias 192.168.13.10
!
alias address-range $TestAddRanAlias 192.168.13.10 to 192.168.13.13
!
alias network-service $NetworkServAlias proto udp
!
alias network-service $kerberos proto tcp 749 750 80 proto udp 68 sourceport
67
!
alias vlan $TestVLANAlias 1
--More--
rfs4000-229D58(config)#

In the follwoing examples the global aliases '$kerberos' and '$TestVLANAlias'
are associated with the RF Domain 'test' and overrides applied:

rfs4000-229D58(config-rf-domain-test)#alias network-service $kerberos proto
tcp
749 750 80

rfs4000-229D58(config-rf-domain-test)#alias vlan $TestVLANAlias 10
```

```
rfs4000-229D58(config-rf-domain-test)#show context
rf-domain test
 no country-code
 alias network-service $kerberos proto tcp 749 750 80
  alias vlan $TestVLANAlias 10
rfs4000-229D58(config-rf-domain-test)#

nx9500-6C8809(config-rf-domain-test)#alias string $test motorolasolutions.com

nx9500-6C8809(config-rf-domain-test)#show context
rf-domain test
 no country-code
 alias string $test motorolasolutions.com
nx9500-6C8809(config-rf-domain-test)#

Example 1:
```

In the following examples, the network-group alias ‘$test’ is configured to include hosts 192.168.1.10 and 192.168.1.11, networks 192.168.2.0/24 and 192.168.3.0/24 and address-range 192.168.4.10 to 192.168.4.20.

```
rfs4000-229D58(config)#alias network-group $test host 192.168.1.10
192.168.1.11
rfs4000-229D58(config)#alias network-group $test network 192.168.2.0/24
192.168.3.0/24
rfs4000-229D58(config)#alias network-group $test address-range 192.168.4.10 to
192.168.4.20
```

Let us associate this network-group alias ‘$test’ to the RF Domain ‘test’ and override the ‘host’ element of the alias.

```
rfs4000-229D58(config-rf-domain-test)#alias network-group $test host
192.168.10.10
rfs4000-229D58(config-rf-domain-test)#show context
rf-domain test
 no country-code
 alias network-service $kerberos proto tcp 749 750 80
  alias network-group $test host 192.168.10.10
  alias network-group $test network 192.168.2.0/24 192.168.3.0/24
  alias network-group $test address-range 192.168.4.10 to 192.168.4.20
  alias vlan $TestVLANAlias 10
rfs4000-229D58(config-rf-domain-test)#
In the preceding example, the ‘host’ element of the network-group alias
‘$test’ has been overridden. But the ‘network’ and ‘address-range’ elements
have been retained as is.
```

Related Commands:

no	Removes a network, network-group, network-service, VLAN, or string alias from this RF Domain

channel-list

rf-domain-mode commands

Configures the channel list advertised by radios. This command also enables a dynamic update of a channel list

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
channel-list [2.4GHz|5GHz|dynamic]

channel-list dynamic

channel-list [2.4GHz|5GHz] <CHANNEL-LIST>
```

Parameters

```
channel-list dynamic
```

dynamic	Enables a dynamic update of a channel list

```
channel-list [2.4GHz|5GHz] <CHANNEL-LIST>
```

2.4GHz <CHANNEL-LIST>	Configures the channel list advertised by radios operating in the 2.4 GHz mode • <CHANNLE-LIST> – Specify the list of channels separated by commas or hyphens.
5GHz <CHANNEL-LIST>	Configures the channel list advertised by radios operating in the 5.0 GHz mode • <CHANNLE-LIST> – Specify the list of channels separated by commas or hyphens.

Example

```
rfs7000-37FABE(config-rf-domain-default)#channel-list 2.4GHz 1-10

rfs7000-37FABE(config-rf-domain-default)#show context
rf-domain default
 no country-code
 channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
rfs7000-37FABE(config-rf-domain-default)#
```

Related Commands:

no	Removes the list of channels configured on the selected RF Domain for 2.4 GHz and 5.0 GHz bands. Also disables dynamic update of a channel list.

contact

rf-domain-mode commands

Configures the network administrator's contact details. The network administrator is responsible for addressing problems impacting the network.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
contact <WORD>
```

Parameters

```
contact <WORD>
```

contact <WORD>	Specify contact details, such as name and number.

Example

```
rfs7000-37FABE(config-rf-domain-default)#contact Bob+919621212577

rfs7000-37FABE(config-rf-domain-default)#show context
rf-domain default
 contact Bob+919621212577
 no country-code
 channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
rfs7000-37FABE(config-rf-domain-default)#
```

Related Commands:

no	Removes a network administrator's contact details

control-vlan

rf-domain-mode commands

Configures the VLAN designated for traffic control in this RF Domain

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
control-vlan <1-4094>
```

Parameters

```
control-vlan <1-4094>
```

<1-4094>	Specify the VLAN ID from 1 - 4094. The default is 1.

Example

```
rfs7000-37FABE(config-rf-domain-default)#control-vlan 1

rfs7000-37FABE(config-rf-domain-default)#show context
rf-domain default
 contact Bob+919621212577
 no country-code
```

```
 channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
 control-vlan 1
rfs7000-37FABE(config-rf-domain-default)#
```

Related Commands:

no	Disables the VLAN designated for controlling RF Domain traffic

controller-managed

rf-domain-mode commands

Configures the adopting controller (wireless controller, access point, or service platform) as this RF Domain's manager. In other words, the RF Domain is controller managed, and the managing controller is the device managing the RF Domain.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
controller-managed
```

Parameters

None

Example

```
rfs4000-229D58(config-rf-domain-test)#controller-managed
rfs4000-229D58(config-rf-domain-test)#commit

rfs4000-229D58(config-rf-domain-test)#show context
rf-domain test
 country-code in
 controller-managed
 network-alias techPubs host 192.168.13.8
 network-alias techPubs address-range 192.168.13.10 to 192.168.13.15
 service-alias testing index 10 proto 9 destination-port range 21 21
rfs4000-229D58(config-rf-domain-test)#
```

Related Commands:

no	Removes the adopting controller or service platform as this RF Domain's manager

country-code

rf-domain-mode commands

Configures a RF Domain's country of operation. Since device channels transmit in specific channels unique to the country of operation, it is essential to configure the country code correctly or risk using illegal operation.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
country-code <WORD>
```

Parameters

```
country-code <WORD>
```

country-code	Configures the RF Domain's country of operation
<WORD>	Specify the two (2) letter ISO-3166 country code.

Example

```
rfs7000-37FABE(config-rf-domain-default)#country-code in

rfs7000-37FABE(config-rf-domain-default)#show context
rf-domain default
 contact Bob+919621212577
 country-code in
 channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
 control-vlan 1
rfs7000-37FABE(config-rf-domain-default)#
```

Related Commands:

no	Removes the country of operation configured on a RF Domain

layout

rf-domain-mode commands

Configures the RF Domain layout in terms of area, floor, and location on a map. It allows users to place APs across the deployment map. A maximum of 256 layouts is permitted.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
layout [area|floor|map-location]
layout area <AREA-NAME> {(floor|map-location)}
layout floor <FLOOR-NAME>{(<1-4094>|area|maplocation)}
```

```
layout map-location <URL> units [feet|meters] {(area <AREA-NAME>|floor
<FLOOR-NAME>)}
```

Parameters

```
layout area <AREA-NAME> {(floor|map-location)}
```

layout	Configures the RF Domain's layout in terms of area, floor, and location on a map
area <AREA-NAME>	Configures the RF Domain's area name • <AREA-NAME> – Specify the area name. After configuring the RF Domain's area of functioning, optionally specify the floor name (and number), and/or the map location.

```
layout floor <FLOOR-NAME>{(<1-4094>|area|maplocation)}
```

layout	Configures the RF Domain's layout in terms of area, floor, and location on a map
floor <FLOOR-NAME> <1-4094>	Configures the RF Domain's floor name • <FLOOR-NAME> – Specify the floor name. • <1-4094> – Optional. Specifies the floor number from 1 - 4094. The default floor number is 1. After configuring the RF Domain's floor name (and number), optionally specify the area name and/or the map location.

```
layout map-location <URL> units [feet|meters] {(area <AREA-NAME>|floor
<FLOOR-NAME>)}
```

layout	Configures the RF Domain's layout in terms of area, floor, and location on the map
map-location <URL> units [feet|meters]	Configures the location of the RF Domain on the map • <URL> – Specify the URL to configure the map location. **NOTE:** units [feet|meters] – Configures the map units in terms of feet or meters
area <AREA-NAME>	Optional. Configures the RF Domain's area name. Specify area name. After configuring the RF Domain's area name, optionally specify the floor name and number
floor <FLOOR-NAME>	Optional. Configures the RF Domain's floor name. Specify floor name. After configuring the floor name (and number) for this RF Domain, optionally specify the area name.

Example

```
rfs7000-37FABE(config-rf-domain-default)#layout map-location
www.firstfloor.com units meters area Ecospace floor Floor5

rfs7000-37FABE(config-rf-domain-default)#show context
rf-domain default
 contact Bob+919621212577
 country-code in
 channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
 layout area Ecospace floor Floor5 map-location www.fiestfloor.com units
meters
 control-vlan 1
rfs7000-37FABE(config-rf-domain-default)#
```

Related Commands:

no	Removes the RF Domain layout details

location

rf-domain-mode commands

Configures the RF Domain's physical location. The location could be as specific as the building name or floor number. Or it could be generic and include an entire site. The location defines the physical area where a common set of device configurations are deployed and managed by a RF Domain policy.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
location <WORD>
```

Parameters

```
location <WORD>
```

location <WORD>	Configures the RF Domain location by specifying the area or building name • <WORD> – Specify the location.

Example

```
rfs7000-37FABE(config-rf-domain-default)#location SanJose

rfs7000-37FABE(config-rf-domain-default)#show context
rf-domain default
 location SanJose
 contact Bob+919621212577
 country-code in
 channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
 layout area Ecospace floor Floor5 map-location www.fiestfloor.com units
meters
 control-vlan 1
rfs7000-37FABE(config-rf-domain-default)#
```

Related Commands:

no	Removes the RF Domain location

mac-name

rf-domain-mode commands

Configures a relevant name for each MAC address

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
mac-name <MAC> <NAME>
```

Parameters

```
mac-name <MAC> <NAME>
```

mac-name	Configures a relevant name for each MAC address
<MAC> <NAME>	Specifies the MAC address • <NAME> – Specify a friendly name for this MAC address to use in events and statistics.

Example

```
rfs7000-37FABE(config-rf-domain-default)#mac-name 11-22-33-44-55-66
TestDevice

rfs7000-37FABE(config-rf-domain-default)#show context
rf-domain default
 location SanJose
 contact Bob+919621212577
 country-code in
 channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
 mac-name 11-22-33-44-55-66 TestDevice
 layout area Ecospace floor Floor5 map-location www.fiestfloor.com units
meters
 control-vlan 1
rfs7000-37FABE(config-rf-domain-default)#
```

Related Commands:

no	Removes the MAC address to name mapping

no

rf-domain-mode commands

Negates a command or reverts configured settings to their default. When used in the config RF Domain mode, the no command negates or reverts RF Domain settings.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no
[alias|channel-list|contact|control-vlan|controller-managed|country-code|layo
ut|

location|mac-name|override-smartrf|override-wlan|sensor-server|stats|timezone
|
          tree-node|use]
```

Parameters

```
no
[alias|channel-list|contact|control-vlan|controller-managed|country-code|layo
ut|
location|mac-name|override-smartrf|override-wlan|sensor-server|stats|timezone
|
tree-node|use]
```

no alias	Removes aliases associated with this RF Domain
no channel-list	Removes the channel list for the 2.4 GHz and 5.0 GHz bands. Also disables dynamic update of a channel list.
no contact	Removes configured contact details
no control-vlan	Removes the VLAN configured for controlling traffic
no controller-managed	Removes the adopting controller (access point, wireless controller, or service platform) as this RF Domain's manager
no country-code	Removes the country of operation configured
no layout	Removes RF Domain layout details
no location	Removes RF Domain location details
no mac-name	Removes the MAC address to name mapping
no override-smartrf	Resets override Smart RF settings to default
no override-wlan	Resets override WLAN settings to default
no sensor-server	Disables AirDefense sensor server details
no stats	Resets RF Domain stats settings
no timezone	Removes RF Domain's time zone
no tree-node	Removes the configured hierarchial (tree-node) structure under which this RF Domain appears
no use	Resets RF Domain profile settings

Example

```
The following example shows the default RF Domain settings before the 'no'
commands are executed:

rfs7000-37FABE(config-rf-domain-default)#show context
rf-domain default
 location SanJose
 contact Bob+919621212577
 country-code in
 channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
 mac-name 11-22-33-44-55-66 TestDevice
 layout area Ecospace floor Floor5 map-location www.fiestfloor.com units
meters
 control-vlan 1
rfs7000-37FABE(config-rf-domain-default)#

rfs7000-37FABE(config-rf-domain-default)#no channel-list 2.4GHz 1-10
rfs7000-37FABE(config-rf-domain-default)#no mac-name 11-22-33-44-55-66
rfs7000-37FABE(config-rf-domain-default)#no location
rfs7000-37FABE(config-rf-domain-default)#no control-vlan

The following example shows the default RF Domain settings after the 'no'
commands are executed:
```

```
rfs7000-37FABE(config-rf-domain-default)#show context
rf-domain default
 contact Bob+919621212577
 country-code in
 layout area Ecospace floor Floor5 map-location www.fiestfloor.com units
meters
rfs7000-37FABE(config-rf-domain-default)#
```

Related Commands:

alias	Configures network, VLAN, and service aliases at the RF Domain level
channel-list	Configures the channel list advertised by radios, and enables dynamic update of channel lists
contact	Configures details of the person to contact (or the administrator) in case of any problems or issues impacting the RF Domain
control-vlan	Configures a VLAN for traffic control
controller-managed	Configures the adopting controller or service platform as this RF Domain's manager
country-code	Configures a RF Domain's country of operation
layout	Configures a RF Domain's layout maps
location	Configures a RF Domain's deployment location
mac-name	Configures a relevant name for each MAC address
override-smart-rf	Configures RF Domain level overrides for Smart RF
override-wlan	Configures RF Domain level overrides for WLAN
sensor-server	Configures an AirDefense sensor server
stats	Configures RF Domain stats settings
timezone	Configures a RF Domain's geographic time zone
tree-node	Configures the hierarchial (tree-node) structure under which this RF Domain appears
use	Enables the use of a Smart RF and/or WIPS policy

override-smart-rf

rf-domain-mode commands

Enables dynamic channel switching for Smart RF radios

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
override-smartrf channel-list [2.4GHz|5GHZ] <CHANNEL-LIST>
```

Parameters

```
override-smartrf channel-list [2.4GHz|5GHZ] <CHANNEL-LIST>
```

override-smartrf	Enables dynamic channel switching for Smart RF radios
channel-list	Configures a list of channels for 2.4 GHz and 5.0 GHz Smart RF radios
2.4GHz <CHANNEL-LIST>	Selects the 2.4 GHz Smart RF radio channels • <CHANNEL-LIST> – Specify a list of channels separated by commas.
5GHz <CHANNEL-LIST>	Selects the 5.0 GHz Smart RF radio channels • <CHANNEL-LIST> – Specify a list of channels separated by commas.

Example

```
rfs7000-37FABE(config-rf-domain-default)#override-smartrf channel-list 2.4GHz
1,2,3

rfs7000-37FABE(config-rf-domain-default)#show context
rf-domain default
 contact Bob+919621212577
 country-code in
 override-smartrf channel-list 2.4GHz 1,2,3
 layout area Ecospace floor Floor5 map-location www.fiestfloor.com units
meters
rfs7000-37FABE(config-rf-domain-default)#
```

Related Commands:

no	Resets the override Smart RF settings its default

override-wlan

rf-domain-mode commands

Configures RF Domain level overrides for a WLAN

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
overrides-wlan <WLAN> [ssid|vlan-pool|wpa-wpa2-psk]

overrides-wlan <WLAN> [ssid <SSID>|vlan-pool <1-4094> {limit <0-8192>}|
          wpa-wpa2-psk <PASSPHRASE>]
```

Parameters

```
overrides-wlan <WLAN> [ssid <SSID>|vlan-pool <1-4094> {limit
<0-8192>}|wpa-wpa2-psk <PASSPHRASE>]
```

<WLAN>	Configures the WLAN name The name should not exceed 32 characters and should represent the WLAN coverage area. After creating the WLAN, configure its override parameters.
ssid <SSID>	Configures a override SSID associated with this WLAN The SSID should not exceed 32 characters.
vlan-pool <1-4094> {limit <0-8192>}	Configures the override VLANs available to this WLAN • <1-4094> – Specify the VLAN ID from 1 - 4094. • limit <0-8192> – Optional. Sets a limit to the number of users on this VLAN from 0 - 8192. The default is 0.
wpa-wpa2-psk <PASSPHRASE>	Configures the WPA-WPA2 pre-shared key or passphrase for this WLAN • <PASSPHRASE> – Specify a WPA-WPA2 key or passphrase.

Example

```
rfs7000-37FABE(config-rf-domain-default)#override-wlan test vlan-pool 2 limit
20

rfs7000-37FABE(config-rf-domain-default)#show context
rf-domain default
 contact Bob+919621212577
 country-code in
 override-smartrf channel-list 2.4GHz 1,2,3
 override-wlan test vlan-pool 2 limit 20
 layout area Ecospace floor Floor5 map-location www.fiestfloor.com units
meters
rfs7000-37FABE(config-rf-domain-default)#
```

Related Commands:

no	Resets the override WLAN settings its default

sensor-server

rf-domain-mode commands

Configures an AirDefense sensor server on this RF Domain. Sensor servers allow network administrators to monitor and download data from multiple sensors remote locations using Ethernet TCP/IP or serial communications. This enables administrators to respond quickly to interferences and coverage problems.

The Brocade *Wireless Intrusion Protection System* (WIPS) protects the controller managed network, wireless clients and access point radio traffic from attacks and unauthorized access. WIPS provides tools for standards compliance and around-the-clock wireless network security in a distributed environment. WIPS allows administrators to identify and accurately locate attacks, rogue devices and network vulnerabilities in real time and permits both a wired and wireless lockdown of wireless device connections upon acknowledgement of a threat.

In addition to dedicated Brocade AirDefense sensors, an access point radio can function as a sensor and upload information to a dedicated WIPS server (external to the controller). Unique WIPS server configurations can be used by RF Domains to ensure a WIPS server configuration is available to support the unique data protection needs of individual RF Domains.

WIPS is not supported on a WLAN basis, rather sensor functionality is supported on the access point radio(s) available to each controller managed WLAN. When an access point radio is functioning as a WIPS sensor, it is able to scan in sensor mode across all legal channels within the 2.4 and 5.0 GHz bands. Sensor support requires a Brocade AirDefense WIPS Server on the network. Sensor functionality is not provided by the access point alone. The access point works in conjunction with a dedicated WIPS server

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
sensor-server <1-3> ip <IP> {port [443|8443|<1-65535>]}
```

Parameters

```
sensor-server <1-3> ip <IP> {port [443|8443|<1-65535>]}
```

Sensor-server <1-3>	Configures an AirDefense sensor server parameters • <1-3> – Select the server ID from 1 - 3. The server with the lowest defined ID is reached first. The default is 1.
ip <IP>	Configures the (non DNS) IP address of the sensor server • <IP> – Specify the IP address of the sensor server.
port [443|8443|<1-65535>]	Optional. Configures the sensor server port. The options are: • 443 – Configures port 443, the default port used by the AirDefense server • 8843 – Configures port 883, the default port used by advanced WIPS • <1-6553> – Allows you to select a WIPS/AirDefense sensor server port from 1 - 65535

Example

```
rfs7000-37FABE(config-rf-domain-default)#sensor-server 2 ip 172.16.10.3 port
443

rfs7000-37FABE(config-rf-domain-default)#show context
rf-domain default
 contact Bob+919621212577
 country-code in
 sensor-server 2 ip 172.16.10.3
 override-smartrf channel-list 2.4GHz 1,2,3
 override-wlan test vlan-pool 2 limit 20
 layout area Ecospace floor Floor5 map-location www.fiestfloor.com units
meters
rfs7000-37FABE(config-rf-domain-default)#
```

Related Commands:

no	Disables an AirDefense sensor server parameters

stats

rf-domain-mode commands

Configures stats settings that define how RF Domain statistics are updated

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
stats [open-window|update-interval]

stats open-window <1-2> {sample-interval <5-86640>} {size <3-100>}

stats update-interval [<5-300>|auto]
```

Parameters

```
stats open-window <1-2> {sample-interval <5-86640>} {size <3-100>}
```

stats	Configures stats related settings on this RF Domain
open-window <1-2>	Opens a stats window to get trending data • <1-2> – Configures a numerical index ID for this RF Domain statistics
sample-interval <5-86640>	Optional. Configures the interval at which the wireless controller captures statistics supporting this RF Domain • <5-86640> – Specify the sample interval from 5 - 86640 seconds. The default is 5 seconds.
size <3-100>	Optional. After specifying the interval time, specify the number of samples used to define RF Domain statistics. • <3-100> – Specify the number of samples from 3 - 100. The default is 6 samples.

```
stats update-interval [<5-300>|auto]
```

stats	Configures stats related settings on this RF Domain
update-interval [<5-300>|auto]	Configures the interval at which RF Domain statistics are updated. The options are: • <5-300> – Specify an update interval from 5 - 300 seconds. • auto – The RF Domain manager automatically adjusts the update interval based on the load.

Example

```
rfs7000-37FABE(config-rf-domain-default)#stats update-interval 200
rfs7000-37FABE(config-rf-domain-default)#show context
rf-domain default
 contact Bob+919621212577
 stats update-interval 200
 country-code in
 sensor-server 2 ip 172.16.10.3
 override-smartrf channel-list 2.4GHz 1,2,3
 override-wlan test vlan-pool 2 limit 20
 layout area Ecospace floor Floor5 map-location www.fiestfloor.com units
meters
rfs7000-37FABE(config-rf-domain-default)#
```

Related Commands:

no	Resets stats related settings

timezone

rf-domain-mode commands

Configures the RF Domain's geographic time zone. Configuring the time zone is essential for RF Domains deployed across different geographical locations.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
timezone <TIMEZONE>
```

Parameters

```
timezone <TIMEZONE>
```

time <TIMEZONE>	Specify the RF Domain's time zone.

Example

```
rfs7000-37FABE(config-rf-domain-default)#timezone America/Los_Angeles

rfs7000-37FABE(config-rf-domain-default)#show context
rf-domain default
 contact Bob+919621212577
 timezone America/Los_Angeles
 stats update-interval 200
 country-code in
 sensor-server 2 ip 172.16.10.3
 override-smartrf channel-list 2.4GHz 1,2,3
 override-wlan test vlan-pool 2 limit 20
 layout area Ecospace floor Floor5 map-location www.fiestfloor.com units
meters
rfs7000-37FABE(config-rf-domain-default)#
```

Related Commands:

no	Removes a RF Domain's time zone

tree-node

rf-domain-mode commands

Configures the hierarchial (tree-node) structure under which this RF Domain is located

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
tree-node [campus|city|country|region] {(campus|city|country|region)}
```

Parameters

```
tree-node [campus|city|country|region] {(campus|city|country|region)}
```

tre-node	Configures the hierarchial tree structure defining the RF Domain's location. The tree node hierarchy can be configured in any order, but will always appear as: country > region > city > campus. Further, a higher node, such as country, cannot be defined under a lower node, such as region. An RF Domain can be placed under any one of the tree nodes. But, an RF Domain at the country level may have all four nodes defined. Where as, an RF Domain restricted to a campus, cannot have the country, city, and region nodes. At least one of these four nodes must be defined. This feature is disabled by default.
campus	Configures the campus name for this RF Domain
city	Configures the city for this RF Domain
country	Configures the country for this RF Domain
region	Configures the region for this RF Domain

Usage Guidelines:

The following points need to be taken into consideration when creating the tree-node structure:

- Adding a *country* first is a good idea since *region*, *city*, and *campus* can all be added as sub-nodes in the tree structure. However, the selected country is an invalid tree node until a RF Domain is mapped.
- A city and campus can be added in the tree structure as sub-nodes under a region. An RF Domain can be mapped anywhere down the hierarchy for a region and not just directly under a country. For example, a region can have city, campus, and one RF Domain mapped.
- Only a campus can be added as a sub-node under a city. The city is an invalid tree node until a RF Domain is mapped somewhere within the directory tree.
- A campus is the last node in the hierarchy before a RF Domain, and it is not valid unless it has a RF Domain mapped.
- After creating the tree structure do a *commit* and *save* for the tree configuration to take effect and persist across reboots.

Example

```
rfs4000-229D58(config-rf-domain-test)#tree-node campus EcoSpace City Bangalore
country India region South
rfs4000-229D58(config-rf-domain-test)#

rfs4000-229D58(config-rf-domain-test)#show context
rf-domain test
 country-code in
 tree-node country India region South city Bangalore campus EcoSpace
rfs4000-229D58(config-rf-domain-test)#
```

Related Commands:

no	Removes the RF Domain's tree-node configuration

use

rf-domain-mode commands

Enables the use of Smart RF and WIPS with this RF Domain

Assigns an existing *Wireless IPS* (WIPS) policy to the RF Domain

A WIPS policy provides protection against wireless threats and acts as a key layer of security complementing wireless VPNs, encryption and authentication. A WIPS policy uses a dedicated sensor for actively detecting and locating rogue AP devices. After detection, WIPS uses mitigation techniques to block the devices by manual termination, air lockdown, or port suppression

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
use [smart-rf-policy|wips-policy]

use [smart-rf-policy <SMART-RF-POLICY-NAME>|wips-policy <WIPS-POLICY-NAME>]
```

Parameters

```
use [smart-rf-policy <SMART-RF-POLICY-NAME>|wips-policy <WIPS-POLICY-NAME>]
```

use	Uses a Smart RF policy with this RF Domain
smart-rf-policy <SMART-RF-POLICY-NAME>	Specifies a Smart RF policy • <SMART-RF-POLICY-NAME> – Specify the Smart RF policy name. For more information on configuring smart RF policy, see *SMART-RF-POLICY*.
wips-policy <WIPS-POLICY-NAME>	Specifies a WIPS policy • <WIPS-POLICY-NAME> – Specify the WIPS policy name. For more information on configuring WIPS policy, see *WIPS-POLICY*.

Example

```
rfs7000-37FABE(config-rf-domain-default)#use smart-rf-policy Smart-RF1
rfs7000-37FABE(config-rf-domain-default)#use wips-policy WIPS1

rfs7000-37FABE(config-rf-domain-default)#show context
rf-domain default
 contact Bob+919621212577
 timezone America/Los_Angeles
 stats update-interval 200
 country-code in
        use smart-rf-policy Smart-RF1
 use wips-policy WIPS1
 sensor-server 2 ip 172.16.10.3
 override-smartrf channel-list 2.4GHz 1,2,3
```

```
 override-wlan test vlan-pool 2 limit 20
 layout area Ecospace floor Floor5 map-location www.fiestfloor.com units
meters
rfs7000-37FABE(config-rf-domain-default)#
```

Related Commands:

no	Resets profiles used with this RF Domain
sensor-server	Configures an AirDefense sensor server on this RF Domain
wips-policy	Configures a WIPS policy
smart-rf-policy	Configures a Smart RF policy

rfs4000

Global Configuration Commands

Adds an Brocade Mobility RFS4000 wireless controller to the network

Supported in the following platforms:

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
rfs4000 <DEVICE-Brocade Mobility RFS4000-MAC>
```

Parameters

```
rfs4000 <DEVICE-Brocade Mobility RFS4000>
```

<DEVICE-Brocade Mobility RFS4000-MAC>	Specify the Brocade Mobility RFS4000's MAC address.

Example

```
rfs7000-37FABE(config)#rfs4000 10-20-30-40-50-60
rfs7000-37FABE(config-device-10-20-30-40-50-60)#
```

Related Commands:

no	Removes an Brocade Mobility RFS4000 wireless controller from the network

rfs6000

Global Configuration Commands

Adds a Brocade Mobility RFS6000 wireless controller to the network

Supported in the following platforms:

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
rfs6000 <DEVICE-Brocade Mobility RFS6000-MAC>
```

Parameters

```
rfs6000 <DEVICE-Brocade Mobility RFS6000-MAC>
```

<DEVICE-Brocade Mobility RFS6000-MAC>	Specify the Brocade Mobility RFS6000's MAC address.

Example

```
rfs7000-37FABE(config)#rfs6000 11-20-30-40-50-61
rfs7000-37FABE(config-device-11-20-30-40-50-61)#
```

Related Commands:

no	Removes a Brocade Mobility RFS6000 model controller from the network

rfs7000

Global Configuration Commands

Adds a Brocade Mobility RFS7000 wireless controller to the network

Supported in the following platforms:

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
rfs7000 <DEVICE-Brocade Mobility RFS7000-MAC>
```

Parameters

```
rfs7000 <DEVICE-Brocade Mobility RFS7000-MAC>
```

<DEVICE-Brocade Mobility RFS7000-MAC>	Specify the Brocade Mobility RFS7000's MAC address.

Example

```
rfs7000-37FABE(config)#rfs7000 12-20-30-40-50-62
rfs7000-37FABE(config-device-12-20-30-40-50-62)#
```

Related Commands:

no	Removes a Brocade Mobility RFS7000 model controller from the network

role-policy

Global Configuration Commands

Configures a role-based firewall policy

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
role-policy <ROLE-POLICY-NAME>
```

Parameters

```
role-policy <ROLE-POLICY-NAME>
```

<ROLE-POLICY-NAME>	Specify the role policy name. If the policy does not exist, it is created.

Example

```
rfs7000-37FABE(config)#role-policy role1
rfs7000-37FABE(config-role-policy-role1)#?
Role Policy Mode commands:
  default-role     Configuration for Wireless Clients not matching any role
  ldap-deadperiod  Ldap dead period interval
  ldap-server      Add a ldap server
  ldap-service     Enable ldap attributes in role definition
  ldap-timeout     Ldap query timeout interval
  no               Negate a command or set its defaults
  user-role        Create a role

  clrscr           Clears the display screen
  commit           Commit all changes made in this session
  do               Run commands from Exec mode
  end              End current mode and change to EXEC mode
  exit             End current mode and down to previous mode
  help             Description of the interactive help system
  revert           Revert changes
  service          Service Commands
  show             Show running system information
  write            Write running configuration to memory or terminal

rfs7000-37FABE(config-role-policy-role1)#
```

NOTE
For more information on role policy commands, see *Chapter 19, ROLE-POLICY*.

Related Commands:

no	Removes an existing role policy

routing-policy

Global Configuration Commands

Configures a routing policy

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
role-policy <ROUTING-POLICY-NAME>
```

Parameters

```
role-policy <ROUTING-POLICY-NAME>
```

<ROUTING-POLICY-NAME>	Specify the role policy name. If the policy does not exist, it is created.

Example

```
rfs7000-37FABE(config)#routing-policy TestRoutingPolicy
rfs7000-37FABE(config-routing-policy-TestRoutingPolicy)#?
Routing Policy Mode commands:
  apply-to-local-packets  Use Policy Based Routing for packets generated by
                          the device
  logging                 Enable logging for this Route Map
  no                      Negate a command or set its defaults
  route-map               Create a Route Map
  use                     Set setting to use

  clrscr                  Clears the display screen
  commit                  Commit all changes made in this session
  do                      Run commands from Exec mode
  end                     End current mode and change to EXEC mode
  exit                    End current mode and down to previous mode
  help                    Description of the interactive help system
  revert                  Revert changes
  service                 Service Commands
  show                    Show running system information
  write                   Write running configuration to memory or terminal

rfs7000-37FABE(config-routing-policy-TestRoutingPolicy)#
```

NOTE
For more information on routing policy commands, see *Chapter 25, ROUTING-POLICY*.

Related Commands:

no	Removes an existing routing policy

self

Global Configuration Commands

Displays the device's configuration context

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
self
```

Parameters

None

Example

```
rfs7000-37FABE(config)#self
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#
```

smart-rf-policy

Global Configuration Commands

Configures a Smart RF policy

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
smart-rf-policy <SMART-RF-POLICY-NAME>
```

Parameters

```
smart-rf-policy <SMART-RF-POLICY-NAME>
```

<SMART-RF-POLICY-NAME>	Specify the Smart RF policy name. If the policy does not exist, it is created.

Example

```
rfs7000-37FABE(config)#smart-rf-policy test
rfs7000-37FABE(config-smart-rf-policy-test)#?
Smart RF Mode commands:
  area                    Specify channel list/ power for an area
  assignable-power        Specify the assignable power during power-assignment
  channel-list            Select channel list for smart-rf
  channel-width           Select channel width for smart-rf
  coverage-hole-recovery  Recover from coverage hole
  enable                  Enable this smart-rf policy
  group-by                Configure grouping parameters
```

```
  interference-recovery   Recover issues due to excessive noise and
                          interference
  neighbor-recovery       Recover issues due to faulty neighbor radios
  no                      Negate a command or set its defaults
  sensitivity             Configure smart-rf sensitivity (Modifies various
                          other smart-rf configuration items)
  smart-ocs-monitoring    Smart off channel scanning

  clrscr                  Clears the display screen
  commit                  Commit all changes made in this session
  end                     End current mode and change to EXEC mode
  exit                    End current mode and down to previous mode
  help                    Description of the interactive help system
  revert                  Revert changes
  service                 Service Commands
  show                    Show running system information
  write                   Write running configuration to memory or term

rfs7000-37FABE(config-smart-rf-policy-test)#
```

NOTE
For more information on Smart RF policy commands, see *Chapter 20, SMART-RF-POLICY*.

Related Commands:

no	Removes an existing Smart RF policy

wips-policy

Global Configuration Commands

Configures a WIPS policy

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
wips-policy <WIPS-POLICY-NAME>
```

Parameters

```
wips-policy <WIPS-POLICY-NAME>
```

<WIPS-POLICY-NAME>	Specify the WIPS policy name. If the policy does not exist, it is created.

Example

```
rfs7000-37FABE(config)#wips-policy test
rfs7000-37FABE(config-wips-policy-test)#?
Wips Policy Mode commands:
```

```
  br-detection                Rogue AP detection
  enable                      Enable this wips policy
  event                       Configure an event
  history-throttle-duration   Configure the duration for which event duplicates
                              are not stored in history
  interference-event          Specify events which will contribute to smart-rf
                              wifi interference calculations
  no                          Negate a command or set its defaults
  signature                   Signature to configure
  use                         Set setting to use

  clrscr                      Clears the display screen
  commit                      Commit all changes made in this session
  do                          Run commands from Exec mode
  end                         End current mode and change to EXEC mode
  exit                        End current mode and down to previous mode
  help                        Description of the interactive help system
  revert                      Revert changes
  service                     Service Commands
  show                        Show running system information
  write                       Write running configuration to memory or terminal

rfs7000-37FABE(config-wips-policy-test)#
```

NOTE
For more information on WIPS policy commands, see *Chapter 21, WIPS-POLICY*.

Related Commands:

no	Removes an existing WIPS policy

wlan

Global Configuration Commands

Configures a *Wireless Local Area Network* (WLAN)

The following table lists WLAN configuration mode commands.

Command	Description	Reference
wlan	Creates a new wireless LAN and enters its configuration mode	page 315
wlan-mode commands	Summarizes WLAN configuration mode commands	page 318

wlan

wlan

Configures a WLAN and enters its configuration mode. Use this command to modify an existing WLAN's settings.

4

A WLAN is a data-communications system that flexibly extends the functionality of a wired LAN. A WLAN links two or more computers or devices using spread-spectrum or OFDM modulation based technology. WLANs do not require lining up devices for line-of-sight transmission, and are thus, desirable for wireless networking. Roaming users can be handed off from one access point to another, like a cellular phone system. WLANs can therefore be configured around the needs of specific user groups, even when they are not in physical proximity.

WLANs can provide an abundance of services, including data communications (allowing mobile devices to access applications), e-mail, file, and print services or even specialty applications (such as guest access control and asset tracking).

Each WLAN configuration contains encryption, authentication and QoS policies and conditions for user connections. Connected access point radios transmit periodic beacons for each BSS. A beacon advertises the SSID, security requirements, supported data rates of the wireless network to enable clients to locate and connect to the WLAN.

WLANs are mapped to radios on each access point. A WLAN can be advertised from a single access point radio or can span multiple access points and radios. WLAN configurations can be defined to provide service to specific areas of a site. For example, a guest access WLAN may only be mapped to a 2.4 GHz radio in a lobby or conference room providing limited coverage, while a data WLAN is mapped to all 2.4 GHz and 5.0 GHz radios at the branch site to provide complete coverage.

Brocade Mobility RFS4000 and Brocade Mobility RFS6000 controllers support a maximum of 32 WLANs. The Brocade Mobility RFS7000 model wireless controller supports up to 256 WLANs. An access point supports a maximum of 16 WLANs.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
wlan {<WLAN-NAME>|containing <WLAN-NAME>}
```

Parameters

```
wlan {<WLAN-NAME>|containing <WLAN-NAME>}
```

wlan <WLAN-NAME>	Configures a new WLAN • <WLAN-NAME> – Optional. Specify the WLAN name. The WLAN name could be a logical representation of its coverage area (for example, engineering, marketing etc.).The name cannot exceed 32 characters.
containing <WLAN-NAME>	Optional. Configures an existing WLAN's settings • <WLAN-NAME> – Specify a sub-string in the WLAN name. Use this parameter to filter a WLAN. This option allows you to select and enter the configuration mode of one or more WLANs.

Example

```
rfs7000-37FABE(config)#wlan 1
rfs7000-37FABE(config-wlan-1)#

rfs7000-37FABE(config)#wlan containing wlan1
rfs7000-37FABE(config-wlan-{'containing': 'wlan1'})#
```

```
rfs7000-37FABE(config-wlan-1)#?
Wireless LAN Mode commands:
  accounting                            Configure how accounting records are
                                        created for this wlan
  acl                                   Actions taken based on ACL
                                        configuration [packet drop being one
                                        of them]
  answer-broadcast-probes               Include this wlan when responding to
                                        probe requests that do not specify an
                                        SSID
  association-list                      Configure the association list for
                                        the wlan
  authentication-type                   The authentication type of this WLAN
  bridging-mode                         Configure how packets to/from this
                                        wlan are bridged
  broadcast-dhcp                        Configure broadcast DHCP packet
                                        handling
  broadcast-ssid                        Advertise the SSID of the WLAN in
                                        beacons
  captive-portal-enforcement            Enable captive-portal enforcement on
                                        the wlan
  client-access                         Enable client-access (normal data
                                        operations) on this wlan
  client-client-communication           Allow switching of frames from one
                                        wireless client to another on this
                                        wlan
  client-load-balancing                 Configure load balancing of clients
                                        on this wlan
  controller-assisted-mobility          Enable controller assisted mobility
                                        to determine wireless clients' VLAN
                                        assignment
  data-rates                            Specify the 802.11 rates to be
                                        supported on this wlan
  description                           Configure a description of the usage
                                        of this wlan
  downstream-group-addressed-forwarding Enable downstream group addressed
                                        forwarding of packets
  dynamic-vlan-assignment               Dynamic VLAN assignment configuration
  eap-types                             Configure client access based on
                                        eap-type used for authentication
  encryption-type                       Configure the encryption to use on
                                        this wlan
  enforce-dhcp                          Drop packets from Wireless Clients
                                        with static IP address
  fast-bss-transition                   Configure support for 802.11r Fast
                                        BSS Transition
  http-analyze                          Enable HTTP URL analysis on the wlan
  ip                                    Internet Protocol (IP)
  kerberos                              Configure kerberos authentication
                                        parameters
  mac-authentication                    Configure mac-authentication related
                                        parameters
  mac-registration                      Enable dynamic MAC registration of
                                        user
  motorola-extensions                   Enable support for Motorola-Specific
                                        extensions to 802.11
  no                                    Negate a command or set its defaults
  protected-mgmt-frames                 Protected Management Frames (IEEE
```

```
                                        802.11w) related configuration (DEMO
                                        FEATURE)
  proxy-arp-mode                        Configure handling of ARP requests
                                        with proxy-arp is enabled
  radio-resource-measurement            Configure support for 802.11k Radio
                                        Resource Measurement
  radius                                Configure RADIUS related parameters
  relay-agent                           Configure dhcp relay agent info
  shutdown                              Shutdown this wlan
  ssid                                  Configure the Service Set Identifier
                                        for this WLAN
  time-based-access                     Configure client access based on time
  use                                   Set setting to use
  vlan                                  Configure the vlan where traffic from
                                        this wlan is mapped
  vlan-pool-member                      Add a member vlan to the pool of
                                        vlans for the wlan (Note:
                                        configuration of a vlan-pool
                                        overrides the 'vlan' configuration)
  wep128                                Configure WEP128 parameters
  wep64                                 Configure WEP64 parameters
  wireless-client                       Configure wireless-client specific
                                        parameters
  wpa-wpa2                              Modify tkip-ccmp (wpa/wpa2) related
                                        parameters

  clrscr                                Clears the display screen
  commit                                Commit all changes made in this
                                        session
  do                                    Run commands from Exec mode
  end                                   End current mode and change to EXEC
                                        mode
  exit                                  End current mode and down to previous
                                        mode
  help                                  Description of the interactive help
                                        system
  revert                                Revert changes
  service                               Service Commands
  show                                  Show running system information
  write                                 Write running configuration to memory
                                        or terminal

rfs7000-37FABE(config-wlan-1)#
```

wlan-mode commands

wlan

This section documents the WLAN configuration mode commands in detail.

Use the (config) instance to configure WLAN related parameters.

To navigate to this instance, use the following command:

```
<DEVICE>(config)#wlan <WLAN-NAME>
```

The following table summarizes WLAN configuration mode commands.

Command	Description	Reference
accounting	Defines a WLAN accounting configuration	page 320
acl	Defines the actions based on an ACL rule configuration	page 322
answer-broadcast-probes	Allows a WLAN to respond to probes for broadcast ESS	page 323
association-list	Attaches an existing global association list to a WLAN	page 324
authentication-type	Sets a WLAN's authentication type	page 324
bridging-mode	Configures how packets to/from this WLAN are bridged	page 326
broadcast-dhcp	Configures broadcast DHCP packet handling	page 326
broadcast-ssid	Advertises a WLAN's SSID in beacons	page 327
captive-portal-enforcement	Configures a WLAN's captive portal enforcement	page 327
client-access	Enables WLAN client access (normal data operations)	page 328
client-client-communication	Allows the switching of frames from one wireless client to another on a WLAN	page 329
client-load-balancing	Enables load balancing of WLAN clients	page 329
controller-assisted-mobility	Enables controller assisted mobility to determine wireless clients' VLAN assignment	page 330
data-rates	Specifies the 802.11 rates supported on the WLAN	page 331
description	Sets a WLAN's description	page 333
downstream-group-addressed-forwarding	Enables forwarding of downstream packets addressed to a group	page 334
dynamic-vlan-assignment	Configures dynamic VLAN assignment on this WLAN	page 335
eap-types	Configures client access based on eap-type used for authentication	page 335
encryption-type	Sets a WLAN's encryption type	page 336
enforce-dhcp	Drops packets from clients with a static IP address	page 337
fast-bss-transition	Configures support for 802.11r fast BSS transition on a WLAN	page 338
http-analyze	Enables HTTP URL analysis on the WLAN	page 339
ip	Configures IP settings	page 340
kerberos	Configures Kerberos authentication parameters	page 341
mac-authentication	Configures MAC authentication parameters	page 343
mac-registration	Enables dynamic MAC registration of user	page 343
motorola-extensions	Enables support for Brocade specific extensions to 802.11	page 345
no	Negates a command or reverts settings to their default	page 346
proxy-arp-mode	Enables the proxy ARP mode for ARP requests	page 349
radio-resource-measurement	Enables support for 802.11k radio resource measurement	page 349
radius	Configures RADIUS parameters	page 350

Command	Description	Reference
relay-agent	Enables support for DHCP relay agent information (option 82) feature on this WLAN	page 351
shutdown	Closes a WLAN	page 352
ssid	Configures a WLAN's SSID	page 353
time-based-access	Configures time-based client access	page 354
use	Defines WLAN mode configuration settings	page 355
vlan	Sets VLAN assignment for a WLAN	page 357
vlan-pool-member	Adds a member VLAN to the pool of VLANs for a WLAN	page 358
wep128	Configures WEP128 parameters	page 359
wep64	Configures WEP64 parameters	page 361
wireless-client	Configures the transmit power for wireless clients transmission	page 362
wpa-wpa2	Modifies TKIP and CCMP (WPA/WPA2) related parameters	page 364
service	Invokes service commands applicable in the WLAN configuration mode	page 366

accounting

wlan-mode commands

Defines the WLAN's accounting configuration

Accounting is the method of collecting user data, such as start and stop times, executed commands (for example, PPP), number of packets and number of bytes received and transmitted. This data is sent to the security server for billing, auditing, and reporting purposes. Accounting enables wireless network administrators to track the services and network resources accessed and consumed by users. When enabled, this feature allows the network access server to report and log user activity to a RADIUS security server in the form of accounting records. Each accounting record is comprised of AV pairs and is stored on the access control server. The data can be analyzed for network management, client billing, and/or auditing. Accounting methods must be defined through AAA policies.

Accounting can be enabled and applied to access point, wireless controller, or service platform managed WLANs. Once enabled, it uniquely logs accounting events specific to the managed WLAN. Accounting logs contain information about the use of remote access services by users. This information is of great assistance in partitioning local versus remote users and how to best accommodate each. Remote user information can be archived to a location outside of the access point for periodic network and user permission administration.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
accounting [radius|syslog|wait-client-ip]
```

```
accounting [radius|wait-client-ip]

accounting syslog [host|mac-address-format]

accounting syslog host <IP/HOSTNAME> {port <1-65535>}
          {proxy-mode [none|through-controller|through-rf-domain-manager]}

accounting syslog mac-address-format
[middle-hyphen|no-delim|pair-colon|pair-hyphen|
          quad-dot] case [lower|upper]
```

Parameters

`accounting [radius|wait-client-ip]`

accounting radius	Enables support for WLAN RADIUS accounting messages. This option is disabled by default. When enabled, the WLAN uses an external RADIUS resource for accounting. Use the use > aaa-policy > <AAA-POLICY-NAME> command to associate an appropriate AAA policy with this WLAN. This AAA policy should be existing and should define the accounting, authentication, and authorization parameters.
accounting wait-client-ip	Enables waiting for client's IP before commencing the accounting procedure

`accounting syslog host <IP/HOSTNAME> {port <1-65535>} {proxy-mode [none|through-controller|through-rf-domain-manager]}`

accounting syslog	Enables support for WLAN syslog accounting messages in standard syslog format (RFC 3164). This option is disabled by default.
host <IP/HOSTNAME>	Configures a syslog destination hostname or IP address for accounting records • <IP/HOSTNAME> – Specify the IP address or name of the destination host.
port <1-65535>	Optional. Configures the syslog server's UDP port (this port is used to connect to the server) • <1-65535> – Specify the port from 1 - 65535. Default port is 514.
proxy-mode [none| through-controller| through-rf-domain-manager]	Optional. Configures the request proxying mode • none – Requests are directly sent to the server from the device • through-controller – Proxies requests through the controller (access point, wireless controller, or service platform) configuring the device • through-rf-domain-manager – Proxies requests through the local RF Domain manager

`accounting syslog mac-address-format [middle-hyphen|no-delim|pair-colon|pair-hyphen|quad-dot] case [lower|upper]`

accounting syslog	Enables support for WLAN syslog accounting messages
mac-address-format	Configures the MAC address format used in syslog messages
middle-hyphen	Configures the MAC address format with middle hyphen (AABBCC-DDEEFF)
no-delim	Configures the MAC address format without delimitors (AABBCCDDEEFF)
pair-colon	Configures the MAC address format with pair-colon delimitors (AA:BB:CC:DD:EE:FF)
pair-hyphen	Configures the MAC address format with pair-hyphen deli mi tors (AA-BB-CC-DD-EE-FF). This is the default setting.
quad-dot	Configures the MAC address format with quad-dot deli mi tors (AABB.CCDD.EEFF)

case [lower|upper]	The following keywords are common to all:
	• case – Specifies MAC address case (upper or lower)
	  • lower – Specifies MAC address is filled in lower case (for example, aa-bb-cc-dd-ee-ff)
	  • upper – Specifies MAC address is filled in upper case (for example, AA-BB-CC-DD-EE-FF)

Example

```
rfs7000-37FABE(config-wlan-test)#accounting syslog host 172.16.10.4 port 2
proxy-mode none

rfs7000-37FABE(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 accounting syslog host 172.16.10.4 port 2
rfs7000-37FABE(config-wlan-test)#
```

acl

wlan-mode commands

Defines the actions taken based on an ACL rule configuration

Use the use > ip-access-list <IP-ACCESS-LIST-NAME> to associate an ACL with the WLAN. The ACL rule is determined by the associated ACL's configuration.

A Firewall is a mechanism enforcing access control, and is considered a first line of defense in protecting proprietary information within the network. The means by which this is accomplished varies, but in principle, a Firewall can be thought of as mechanisms allowing and denying data traffic in respect to administrator defined rules. For an overview of Firewalls, see Wireless Firewall.

WLANs use Firewalls like *Access Control Lists* (ACLs) to filter/mark packets based on the WLAN from which they arrive, as opposed to filtering packets on Layer 2 ports. An ACL contains an ordered list of Access Control Entries (ACEs). Each ACE specifies an action and a set of conditions (rules) a packet must satisfy to match the ACE. The order of conditions in the list is critical since filtering is stopped after the first match.

IP based Firewall rules are specific to source and destination IP addresses and the unique rules and precedence orders assigned. Both IP and non-IP traffic on the same Layer 2 interface can be filtered by applying both an IP ACL and a MAC.

Additionally, administrators can filter Layer 2 traffic on a physical Layer 2 interface using MAC addresses. A MAC Firewall rule uses source and destination MAC addresses for matching operations, where the result is a typical allow, deny or mark designation to WLAN packet traffic.

Keep in mind IP and non-IP traffic on the same Layer 2 interface can be filtered by applying both an IP ACL and a MAC ACL to the interface.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
acl exceed-rate wireless-client-denied-traffic <0-1000000>
{blacklist|disassociate}
```

```
acl exceed-rate wireless-client-denied-traffic <0-1000000> {blacklist
<0-86400>|
          disassociate}
```

Parameters

```
acl exceed-rate wireless-client-denied-traffic <0-1000000> {blacklist
<0-86400>|
disassociate}
```

acl exceed-rate	Sets the actions taken based on an ACL rule configuration (for example, drop a packet) • exceed-rate – Action is taken when the rate exceeds a specified value
wireless-client-denied-traffic <0-1000000>	Sets the action to deny traffic to the wireless client when the rate exceeds the specified value • <0-1000000> – Specify a allowed rate threshold of disallowed traffic in packets/sec.
blacklist <0-86400>	Optional. When enabled, sets the time interval to blacklist a wireless client
disassociate	Optional. When enabled, disassociates a wireless client

Example

```
rfs7000-37FABE(config-wlan-test)#acl exceed-rate
wireless-client-denied-traffic
20 disassociate

rfs7000-37FABE(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 accounting syslog host 172.16.10.4 port 2
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
rfs7000-37FABE(config-wlan-test)#
```

answer-broadcast-probes

wlan-mode commands

Allows the WLAN to respond to probe requests that do not specify a SSID. These probes are for broadcast ESS. This feature is enabled by default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
answer-broadcast-probes
```

Parameters

None

Example

```
rfs7000-37FABE(config-wlan-1)#answer-broadcast-probes
rfs7000-37FABE(config-wlan-1)#
```

association-list

wlan-mode commands

Attaches an existing global association list with this WLAN. For more information on global association lists, see *global-association-list*.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
association-list global <GLOBAL-ASSO-LIST-NAME>
```

Parameters

None

Example

```
rfs4000-229D58(config-wlan-test)#association-list global my-clients
rfs4000-229D58(config-wlan-test)#

rfs4000-229D58(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 association-list global my-clients
rfs4000-229D58(config-wlan-test)#
```

authentication-type

wlan-mode commands

Sets the WLAN's authentication type

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
authentication-type [eap|eap-mac|eap-psk|kerberos|mac|none]
```

Parameters

```
authentication-type [eap|eap-mac|eap-psk|kerberos|mac|none]
```

authentication-type	Configures a WLAN's authentication type The authentication types are: EAP, EAP-MAC, EAP-PSK, Kerberos, MAC, and none.
eap	Configures EAP authentication (802.1X) EAP is the de-facto standard authentication method used to provide secure authenticated access to controller managed WLANs. EAP provides mutual authentication, secured credential exchange, dynamic keying and strong encryption. 802.1X EAP can be deployed with WEP, WPA or WPA2 encryption schemes to further protect user information forwarded over controller managed WLANs. The EAP process begins when an unauthenticated supplicant (client device) tries to connect with an authenticator (in this case, the authentication server). An access point passes EAP packets from the client to an authentication server on the wired side of the access point. All other packet types are blocked until the authentication server (typically, a RADIUS server) verifies the client's identity.
eap-mac	Configures EAP or MAC authentication depending on client. (This setting is valid only with the None encryption type. EAP-MAC is useful when in a hotspot environment, as some clients support EAP and an administrator may want to authenticate based on just the MAC address of the device.
eap-psk	Configures EAP authentication or pre-shared keys depending on client (This setting is only valid with *Temporal Key Integrity Protocol* (TKIP) or *Counter Mode with Cipher Block Chaining Message Authentication Code Protocol* (CCMP) encryption types). When using PSK with EAP, the controller sends a packet requesting a secure link using a pre-shared key. The controller and authenticating device must use the same authenticating algorithm and passcode during authentication. EAP-PSK is useful when transitioning from a PSK network to one that supports EAP.
kerberos	Configures Kerberos authentication (encryption will change to WEP128 if it's not already WEP128 or Keyguard) Kerberos (designed and developed by MIT) provides strong authentication for client/server applications using secret-key cryptography. Using Kerberos, a client must prove its identity to a server (and vice versa) across an insecure network connection. Once a client and server use Kerberos to validate their identity, they encrypt all communications to assure privacy and data integrity. Kerberos can only be used on the Access Point with Brocade 802.11b clients. Kerberos uses *Network Time Protocol* (NTP) for synchronizing the clocks of its *Key Distribution Center* (KDC) server(s).
mac	Configures MAC authentication (RADIUS lookup of MAC address) MAC is a device level authentication method used to augment other security schemes when legacy devices are deployed using static WEP. MAC authentication can be used for device level authentication by permitting WLAN access based on device MAC address. MAC authentication is typically used to augment WLAN security options that do not use authentication (such as static WEP, WPA-PSK and WPA2-PSK) MAC authentication can also be used to assign VLAN memberships, Firewall policies and time and date restrictions. MAC authentication can only identify devices, not users.
none	No authentication is used or the client uses pre-shared keys

Example

```
rfs7000-37FABE(config-wlan-test)#authentication-type eap

rfs7000-37FABE(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode tunnel
 encryption-type none
 authentication-type eap
```

```
 accounting syslog host 172.16.10.4 port 2
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
rfs7000-37FABE(config-wlan-test)#
```

bridging-mode

wlan-mode commands

Configures how packets are bridged to and from a WLAN

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
bridging-mode [local|tunnel]
```

Parameters

```
bridging-mode [local|tunnel]
```

bridging-mode	Configures how packets are bridged to and from a WLAN. The options are local and tunnel.
local	Bridges packets between WLAN and local ethernet ports
tunnel	Tunnels packets to other devices (typically a wireless controller or service platform). This is the default mode.

Example

```
rfs7000-37FABE(config-wlan-test)#bridging-mode local

rfs7000-37FABE(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type eap
 accounting syslog host 172.16.10.4 port 2
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
rfs7000-37FABE(config-wlan-test)#
```

broadcast-dhcp

wlan-mode commands

Configures broadcast DHCP packet parameters

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
broadcast-dhcp validate-offer
```

Parameters

```
broadcast-dhcp validate-offer
```

validate-offer	Validates the broadcast DHCP packet destination (a wireless client associated to the radio) before forwarding over the air

Example

```
rfs7000-37FABE(config-wlan-test)#broadcast-dhcp validate-offer

rfs7000-37FABE(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type eap
 accounting syslog host 172.16.10.4 port 2
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 broadcast-dhcp validate-offer
rfs7000-37FABE(config-wlan-test)#
```

broadcast-ssid

wlan-mode commands

Advertises the WLAN SSID in beacons. This feature is enabled by default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
broadcast-ssid
```

Parameters

None

Example

```
rfs7000-37FABE(config-wlan-1)#broadcast-ssid
rfs7000-37FABE(config-wlan-1)#
```

captive-portal-enforcement

wlan-mode commands

Configures the WLAN's captive portal enforcement

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
captive-portal-enforcement {fall-back}
```

Parameters

```
captive-portal-enforcement {fall-back}
```

captive-portal-enforcement	Enables captive portal enforcement on a WLAN
fall-back	Optional. Enforces captive portal validation if WLAN authentication fails (applicable to EAP or MAC authentication only)

Example

```
rfs7000-37FABE(config-wlan-test)#captive-portal-enforcement fall-back

rfs7000-37FABE(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type eap
 accounting syslog host 172.16.10.4 port 2
 captive-portal-enforcement fall-back
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 broadcast-dhcp validate-offer
rfs7000-37FABE(config-wlan-test)#
```

client-access

wlan-mode commands

Enables WLAN client access (for normal data operations)

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
client-access
```

Parameters

None

Example

```
rfs7000-37FABE(config-wlan-1)#client-access
rfs7000-37FABE(config-wlan-1)#
```

client-client-communication

wlan-mode commands

Allows frame switching from one client to another on a WLAN

This option is enabled by default. It allows clients to exchange packets with other clients. It does not necessarily prevent clients on other WLANs from sending packets to this WLAN, but as long as this setting is also disabled on that WLAN, clients are not permitted to interoperate.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
client-client-communication
```

Parameters

None

Example

```
rfs7000-37FABE(config-wlan-1)#client-client-communication
rfs7000-37FABE(config-wlan-1)#
```

client-load-balancing

wlan-mode commands

Configures client load balancing on a WLAN. This feature is disabled by default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
client-load-balancing {allow-single-band-clients|band-discovery-intvl|
          capability-ageout-time|max-probe-req|probe-req-invl}
```

```
client-load-balancing {allow-single-band-clients [2.4Ghz|5Ghz]|
          band-discovery-intvl <0-10000>|capability-ageout-time <0-10000>}

client-load-balancing {max-probe-req|probe-req-intvl} [2.4Ghz|5Ghz] <0-10000>
```

Parameters

```
client-load-balancing {allow-single-band-clients [2.4Ghz|5Ghz]|
band-discovery-intvl <0-10000>|capability-ageout-time <0-10000>}
```

client-load-balancing	Configures client load balancing on a WLAN
allow-single-band-clients [2.4GHz|5GHz]	Optional. Allows single band clients to associate even during load balancing • 2.4GHz – Enables load balancing across 2.4 GHz channels • 5GHz – Enables load balancing across 5.0 GHz channels
band-discovery-intvl <0-10000>	Optional. Configures the interval to discover a client's band capability before connection • <0-10000> – Specify a value from 0 - 10000 seconds.
capability-ageout-time <0-10000>	Optional. Configures a client's capability ageout interval • <0-10000> – Specify a value from 0 - 10000 seconds.

```
client-load-balancing {max-probe-req|probe-req-intvl} [2.4Ghz|5Ghz] <0-10000>
```

client-load-balancing	Configures WLAN client load balancing
max-probe-req [2.4GHz|5GHz] <0-10000>	Optional. Configures client probe request interval limits for device association • 2.4GHz – Configures maximum client probe requests on 2.4 GHz radios • 5GHz – Configures maximum client probe requests on 5.0 GHz radios • <0-10000> – Specify a client probe request threshold from 0 - 100000.
probe-req-intvl 2.4GHz|5GHz] <0-10000>	Optional. Configures client probe request interval limits for device association • 2.4GHz – Configures the client probe request interval on 2.4 GHz radios • 5GHz – Configures the client probe request interval on 5.0 GHz radios • <0-10000> – Specify a value from 0 - 100000.

Example

```
rfs7000-37FABE(config-wlan-test)#client-load-balancing band-discovery-intvl 2

rfs7000-37FABE(config-wlan-test)#client-load-balancing probe-req-intvl 5ghz 5

rfs7000-37FABE(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type eap
 accounting syslog host 172.16.10.4 port 2
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 captive-portal-enforcement fall-back
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 broadcast-dhcp validate-offer
rfs7000-37FABE(config-wlan-test)#
```

controller-assisted-mobility

wlan-mode commands

Enables controller or service platform assisted mobility to determine a wireless client's VLAN assignment

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
controller-assisted-mobility
```

Parameters

None

Example

```
rfs4000-229D58(config-wlan-test)#controller-assisted-mobility
rfs4000-229D58(config-wlan-test)#

rfs4000-229D58(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 controller-assisted-mobility
rfs4000-229D58(config-wlan-test)#
```

data-rates

wlan-mode commands

Specifies the 802.11 rates supported on a WLAN

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
data-rates [2.4GHz|5GHz]

data-rates 2.4GHz [b-only|bg|bgn|custom|default|g-only|gn]

data-rates 2.4GHz custom [1|11|12|18|2|24|36|48|5.5|54|6|9|basic-1|basic-11|

basic-12|basic-18|basci-2|basic-24|basic-36|basic-48|basic-5.5|basic-54|
          basic-6|basic-9|basic-mcs-1s|mcs-1s|mcs-2s|mcs-3s]

data-rates 5GHz [a-only|an|custom|default]
```

```
data-rates 5GHz custom
[12|18|24|36|48|54|6|9|basic-1|basic-11|basic-12|basic-18|

basic-2|basic-24|basic-36|basic-48|basic-5.5|basic-54|basic-6|basic-9|
          basic-mcs-1s|mcs-1s|mcs2s|mcs3s]
```

Parameters

`data-rates 2.4GHz [b-only|bg|bgn|default|g-only|gn]`

data-rates	Specifies the 802.11 rates supported when mapped to a 2.4 GHz radio
b-only	Uses rates that support only 11b clients
bg	Uses rates that support both 11b and 11g clients
bgn	Uses rates that support 11b, 11g and 11n clients
default	Uses the default rates configured for a 2.4 GHz radio
g-only	Uses rates that support operation in 11g only
gn	Uses rates that support 11g and 11n clients

`data-rates 5GHz [a-only|an|default]`

data-rates	Specifies the 802.11 rates supported when mapped to a 5.0 GHz radio
a-only	Uses rates that support operation in 11a only
an	Uses rates that support 11a and 11n clients
default	Uses default rates configured for a 5.0 GHz

```
data-rates [2.4GHz|5GHz] custom
[1|11|12|18|2|24|36|48|5.5|54|6|9|basic-1|basic-11|
basic-12|basic-18|basic-2|basic-24|basic-36|basic-48|basic-5.5|basic-54|basic
-6|
basic-9|basic-mcs-1s|mcs-1s|mcs-2s|mcs-3s]
```

data-rates [2.4GHz|5GHz]	Specifies the 802.11 rates supported when mapped to a 2.4 GHz or 5.0 GHz radio
custom	Configures a data rates list by specifying each rate individually. Use 'basic-' prefix before a rate to indicate it is used as a basic rate (For example, 'data-rates custom basic-1 basic-2 5.5 11'). The data-rates for 2.4 GHz and 5.0 GHz channels are the same with a few exceptions. The 2.4 GHz channel has a few extra data rates: 1, 11, 2, and 5.5.

1,11,2,5.5	The following data rates are specific to the 2.4 GHz channel: • 1 – 1-Mbps • 11 – 11-Mbps • 2 – 2-Mbps • 5.5 – 5.5-Mbps
[12,18,24,36,48,54,6,9, basic-1,basic-11, basic-12,basic-18, basic-2, basic-36,basic-48, basic-5.5, basic-54,basic-6, basic-9,basic-mcs-1s, mcs-1s,mcs2s,mcs-3s]	The following data rates are common to both the 2.4 GHz and 5.0 GHz channels: • 12 – 12 Mbps • 18 – 18-Mbps • 24 – 24 Mbps • 36 – 36-Mbps • 48 – 48-Mbps • 54 – 54-Mbps • 6 – 6-Mbps • 9 – 9-Mbps • basic-1 – basic 1-Mbps • basic-11 – basic 11-Mbps • basic-12 – basic 12-Mbps • basic-18 – basic 18-Mbps • basic-2 – basic 2-Mbps • basic-36 – basic 36-Mbps • basic-48 – basic 48-Mbps • basic-5.5 – basic 5.5-Mbps • basic-54 – basic 54-Mbps • basic-6 – basic 6-Mbps • basic-9 – basic 9-Mbps • basic-mcs-1s – Modulation and coding scheme data rates for 1 Spatial Stream • mcs-1s – Applicable to 1-spatial stream data rates • mcs-2s – Applicable to 2-spatial stream data rates • mcs-3s – Applicable to 3-spatial stream data rates

Example

```
rfs7000-37FABE(config-wlan-test)#data-rates 2.4GHz gn

rfs7000-37FABE(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type eap
 accounting syslog host 172.16.10.4 port 2
 data-rates 2.4GHz gn
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 captive-portal-enforcement fall-back
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 broadcast-dhcp validate-offer
rfs7000-37FABE(config-wlan-test)#
```

description

wlan-mode commands

Defines the WLAN description

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
description <LINE>
```

Parameters

```
description <LINE>
```

<LINE>	Specify a WLAN description The WLAN's description should help differentiate it from others with similar configurations. The description should not exceed 64 characters.

Example

```
rfs7000-37FABE(config-wlan-test)#description TestWLAN

rfs7000-37FABE(config-wlan-test)#show context
wlan test
 description TestWLAN
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type eap
 accounting syslog host 172.16.10.4 port 2
 data-rates 2.4GHz gn
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 captive-portal-enforcement fall-back
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 broadcast-dhcp validate-offer
rfs7000-37FABE(config-wlan-test)#
```

downstream-group-addressed-forwarding

wlan-mode commands

Enables/disables forwarding of downstream BCMC packets to a group on this WLAN. This feature is enabled by default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
downstream-group-addressed-forwarding
```

Parameters

None

Example

```
rfs4000-229D58(config-wlan-test)#downstream-group-addressed-forwarding
rfs4000-229D58(config-wlan-test)#
```

dynamic-vlan-assignment

wlan-mode commands

Configures dynamic VLAN assignment on this WLAN

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
dynamic-vlan-assignment allowed-vlan <VLAN-ID>
```

Parameters

```
dynamic-vlan-assignment allowed-vlan <VLAN-ID>
```

dynamic-vlan-assignment allowed-vlan	Configures a list of VLAN IDs or VLAN alias allowed access to the WLAN
<VLAN-ID>	Specify the list of VLAN IDs or the VLAN alias names. For example, 10-20, 25, 30-35, $guest. For information on VLAN aliases, see *alias*.

Example

```
rfs4000-229D58(config-wlan-test)#dynamic-vlan-assignment allowed-vlans 10-20
rfs4000-229D58(config-wlan-test)#

rfs4000-229D58(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 dynamic-vlan-assignment allowed-vlans 10-20
rfs4000-229D58(config-wlan-test)#
```

eap-types

wlan-mode commands

Configures client access based on the EAP type used

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
eap-types [allow|deny] [aka|all|fast|peap|sim|tls|ttls]
          {(aka|all|fast|peap|sim|tls|ttls)}
```

Parameters

```
eap-types [allow|deny] [aka|all|fast|peap|sim|tls|ttls]
{(aka|all|fast|peap|sim|tls|ttls)}
```

eap-types [allow|deny]	Configures a list of allowed or denied EAP types • allow – Configures a list of EAP types allowed for WLAN client authentication • deny – Configures a list of EAP types not allowed for WLAN client authentication
[aka|all|fast|peap|sim|tls|ttls]	The following EAP types are common to the 'allow' and 'deny' keywords: • aka – Configures EAP *Authentication and Key Agreement* (AKA) and EAP-AKA' (AKA Prime). EAP-AKA is one of the methods in the EAP authentication framework. It uses *Universal Mobile Telecommunications System* (UMTS) and *Universal Subscriber Identity Module* (USIM) for client authentication and key distribution. • all – Allows or denies usage of all EAP types on the WLAN • fast – Configures EAP *Flexible Authentication via Secure Tunneling* (FAST). EAP-FAST establishes a *Transport Layer Security* (TLS) tunnel, to verify client credentials, using *Protected Access Credentials* (PAC). • peap – Configures *Protected Extensible Authentication Protocol* (PEAP). PEAP or Protected EAP uses encrypted and authenticated TLS tunnel to encapsulate EAP. • sim – Configures EAP *Subscriber Identity Module* (SIM). EAP-SIM uses *Global System for Mobile Communications* (GSMC) SIM for client authentication and key distribution. • tls – Configures EAP *Transport Layer Security* (TLS). EAP-TLS is an EAP authentication method that uses PKI to communicate with a RADIUS server or any other authentication server. • ttls – Configures *Tunneled Transport Layer Security* (TTLS). EAP-TTLS is an extension of TLS. Unlike TLS, TTLS does not require every client to generate and install a CA- signed certificate. **NOTE:** These options are recursive, and more than one EAP type can be selected. The selected options are added to the allowed or denied EAP types list.

Example

```
rfs7000-37FABE(config-wlan-test)#eap-types allow fast sim tls

rfs7000-37FABE(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 eap-types allow fast sim tls
rfs7000-37FABE(config-wlan-test)#
```

encryption-type

wlan-mode commands

Sets a WLAN's encryption type

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
encryption-type
[ccmp|keyguard|none|tkip|tkip-ccmp|wep128|web128-keyguard|wep64]
```

Parameters

```
encryption-type
[ccmp|keyguard|none|tkip|tkip-ccmp|wep128|web128-keyguard|wep64]
```

encryption-type	Configures the WLAN's data encryption parameters
ccmp	Configures *Advanced Encryption Standard* (AES) *Counter Mode CBC-MAC Protocol* (AES-CCM/CCMP)
keyguard	Configures Keyguard-MCM *(Mobile Computing Mode)*
tkip	Configures TKIP
tkip-ccmp	Configures the TKIP and AES-CCM/CCMP encryption modes
wep128	Configures WEP with 128 bit keys
wep128-keyguard	Configures WEP128 as well as Keyguard-MCM encryption modes
wep64	Configures WEP with 64 bit keys. A WEP64 configuration is insecure when two WLANs are mapped to the same VLAN, and one uses no encryption while the other uses WEP.

Example

```
rfs7000-37FABEconfig-wlan-test)#encryption-type tkip-ccmp

rfs7000-37FABE(config-wlan-test)#show context
wlan test
 description TestWLAN
 ssid test
 bridging-mode local
 encryption-type tkip-ccmp
 authentication-type eap
 accounting syslog host 172.16.10.4 port 2
 data-rates 2.4GHz gn
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 captive-portal-enforcement fall-back
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 broadcast-dhcp validate-offer
rfs7000-37FABE(config-wlan-test)#
```

enforce-dhcp

wlan-mode commands

Drops packets from clients with a static IP address

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
enforce-dhcp
```

Parameters

None

Example

```
rfs7000-37FABE(config-wlan-test)#enforce-dhcp

rfs7000-37FABE(config-wlan-test)#show context
wlan test
 description TestWLAN
 ssid test
 bridging-mode local
 encryption-type tkip-ccmp
 authentication-type eap
 accounting syslog host 172.16.10.4 port 2
 data-rates 2.4GHz gn
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 captive-portal-enforcement fall-back
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 enforce-dhcp
 broadcast-dhcp validate-offer
rfs7000-37FABE(config-wlan-test)#
```

fast-bss-transition

wlan-mode commands

Enables or disables support for 802.11r Fast-BSS Transition (FT) on the selected WLAN. This feature is disabled by default.

802.11r is an attempt to undo the burden that security and QoS added to the handoff process, and restore it back to an original four message exchange process. The central application for the 802.11r standard is VOIP using mobile phones within wireless Internet networks. 802.11r FT redefines the security key negotiation protocol, allowing parallel processing of negotiation and requests for wireless resources.

Enabling FT standards provides wireless clients fast, secure and seamless transfer from one base station to another, ensuring continuous connectivity.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
fast-bss-transition
```

Parameters

None

Example

```
rfs7000-37FABE(config-wlan-test)#fast-bss-transition
rfs7000-37FABE(config-wlan-test)#

rfs7000-37FABE(config-wlan-test)#show context
wlan test
 ssid test
 vlan 1
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 fast-bss-transition
rfs7000-37FABE(config-wlan-test)#
```

http-analyze

wlan-mode commands

Enables HTTP URL analysis on the WLAN

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
http-analyze [filter|syslog]
http-analyze filter [images|post|query-string]
http-analyze syslog host <IP/HOSTNAME> {port <1-65535>} {proxy-mode [none|
          through-controller|through-rf-domain-manager]}
```

Parameters

```
http-analyze filter [images|post|query-string]
```

filter	Filters URLs, based on the parameters set, before forwarding them
images	Filters out URLs referring to images (does not forward URL requesting images)
post	Filters out URLs requesting POST (does not forward POST requests). This option is disabled by default.
query-string	Removes query strings from URLs before forwarding them (forwards requests and no data). This option is disabled by default.

```
http-analyze syslog host <IP/HOSTNAME> {port <1-65535>} {proxy-mode [none|
through-controller|through-rf-domain-manager]}
```

syslog host <IP/HOSTNAME>	Forwards client and URL information to a syslog server • host <IP/HOSTNAME> – Specify the syslog server's IP address or hostname
port <1-65535>	Optional. Specifies the UDP port to connect to the syslog server from 1 - 65535
proxy-mode [none| through-controller| through-rf-domain-manager]	Optional. Specifies if the request is to be proxied through another device • none – Requests are sent directly to syslog server from device • through-controller – Proxies requests, to the syslog server, through the controller configuring the device • through-rf-domain-manager – Proxies requests, to the syslog server, through the local RF Domain manager

Example

```
rfs4000-229D58(config-wlan-test)#http-analyze syslog host 192.168.13.10 port
21
proxy-mode through-controller

rfs4000-229D58(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 http-analyze syslog host 192.168.13.10 port 21 proxy-mode through-controller
rfs4000-229D58(config-wlan-test)#
```

ip

wlan-mode commands

Configures *Internet Protocol* (IP) settings

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
ip [arp|dhcp]

ip arp [header-mismatch-validation|trust]

ip dhcp trust
```

Parameters

```
ip arp [header-mismatch-validation|trust]
```

ip arp	Configures the IP settings for ARP packets
header-mismatch-validation	Verifies mismatch of source MAC address in the ARP and Ethernet headers
trust	Sets ARP responses as trusted for a WLAN/range

	`ip dhcp trust`
ip dhcp	Configures the IP settings for DHCP packets
trust	Sets DHCP responses as trusted for a WLAN/range

Example

```
rfs7000-37FABE(config-wlan-test)#ip dhcp trust

rfs7000-37FABE(config-wlan-test)#show context
wlan test
 description TestWLAN
 ssid test
 bridging-mode local
 encryption-type tkip-ccmp
 authentication-type eap
 accounting syslog host 172.16.10.4 port 2
 data-rates 2.4GHz gn
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 captive-portal-enforcement fall-back
 ip dhcp trust
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 enforce-dhcp
 broadcast-dhcp validate-offer
 http-analyze controller
rfs7000-37FABE(config-wlan-test)#
```

kerberos

wlan-mode commands

Configures Kerberos authentication parameters on a WLAN

Kerberos (designed and developed by MIT) provides strong authentication for client/server applications using secret-key cryptography. Using Kerberos, a client must prove its identity to a server (and vice versa) across an insecure network connection.

Once a client and server use Kerberos to validate their identity, they encrypt all communications to assure privacy and data integrity. Kerberos can only be used on the access point with Brocade' 802.11b clients. Kerberos uses *Network Time Protocol* (NTP) for synchronizing the clocks of its *Key Distribution Center* (KDC) server(s).

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
kerberos [password|realm|server]

kerberos password [0 <LINE>|2 <LINE>|<LINE>]

kerberos realm <REALM>
```

```
kerberos server [primary|secondary|timeout]

kerberos server [primary|secondary] host <IP/HOSTNAME> {port <1-65535>}

kerberos server timeout <1-60>
```

Parameters

```
kerberos password [0 <LINE>|2 <LINE>|<LINE>]
```

kerberos	Configures a WLAN's Kerberos authentication parameters The parameters are: password, realm, and server.
password	Configures a Kerberos *Key Distribution Center* (KDC) server password. The password should not exceed 127 characters. The password options are: • 0 <LINE> – Configures a clear text password • 2 <LINE> – Configures an encrypted password • <LINE> – Specify the password.

```
kerberos realm <REALM>
```

kerberos	Configures a WLAN's Kerberos authentication parameters The parameters are: password, realm, and server.
realm <REALM>	Configures a Kerberos KDC server realm. The REALM should not exceed 127 characters.

```
kerberos server [primary|secondary] host <IP/HOSTNAME> {port <1-65535>}
```

kerberos	Configures a WLAN's Kerberos authentication parameters The parameters are: password, realm, and server.
server [primary|secondary]	Configures the primary and secondary KDC server parameters • primary – Configures the primary KDC server parameters • secondary – Configures the secondary KDC server parameters
host <IP/HOSTNAME>	Sets the primary or secondary KDC server address • <IP/HOSTNAME> – Specify the IP address or name of the KDC server.
port <1-65535>	Optional. Configures the UDP port used to connect to the KDC server • <1-65535> – Specify the port from 1 - 65535. The default is 88.

```
kerberos server timeout <1-60>
```

kerberos	Configures a WLAN's Kerberos authentication parameters The parameters are: password, realm, and server.
timeout <1-60>	Modifies the Kerberos KDC server's timeout parameters • <1-60> – Specifies the wait time for a response from the Kerberos KDC server before retrying. Specify a value from 1 - 60 seconds.

Example

```
rfs7000-37FABE(config-wlan-test)#kerberos server timeout 12

rfs7000-37FABE(config-wlan-test)#kerberos server primary host 172.16.10.2 port
88

rfs7000-37FABE(config-wlan-test)#show context
wlan test
 description TestWLAN
 ssid test
 bridging-mode local
```

```
 encryption-type tkip-ccmp
 authentication-type eap
 kerberos server timeout 12
 kerberos server primary host 172.16.10.2
 accounting syslog host 172.16.10.4 port 2
 data-rates 2.4GHz gn
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 captive-portal-enforcement fall-back
 ip dhcp trust
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 enforce-dhcp
 broadcast-dhcp validate-offer
 http-analyze controller
rfs7000-37FABE(config-wlan-test)#
```

mac-authentication

wlan-mode commands

Enables MAC authentication. When enabled, the system uses cached credentials (RADIUS server lookups are skipped) to authenticate clients.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
mac-authentication cached-credentials
```

Parameters

```
mac-authentication cached-credentials
```

mac-authentication cached-credentials	Uses cached credentials to skip RADIUS lookups

Example

```
rfs4000-229D58(config-wlan-test)#mac-authentication cached-credentials
rfs4000-229D58(config-wlan-test)#
```

mac-registration

wlan-mode commands

Enables dynamic MAC registration of a user

NOTE
This feature is supported only if MAC authentication is enabled. To enable MAC authentication use the *authentication-type* > *mac* command in the config WLAN mode.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
mac-registration [external|group-name]
mac-registration external host <IP/HOSTNAME> {proxy-mode
[none|through-controller|
          through-rf-domain-manager]}
mac-registration group-name <GROUP-NAME> {agreement-refresh <0-100>|
          expiry-time <1-1500>}
```

Parameters

```
mac-registration external host <IP/HOSTNAME> {proxy-mode
[none|through-controller|
through-rf-domain-manager]}
```

mac-registration	Enables dynamic MAC registration of a user
external	Forwards MAC registration user information to the external controller
host <IP/HOSTNAME>	Specifies the external controller's IP address or hostname
proxy-mode {none| through-controller| through-rf-domain}	Optional. Specifies the forwarding mode • none – Requests are sent directly to the controller from the requesting device • through-controller – Requests are proxied through the controller configuring the device • through-rf-domain – Requests are proxied through the local RF Domain manager

```
mac-registration group-name <GROUP-NAME> {agreement-refresh <0-100>|
expiry-time <1-1500>}
```

mac-registration	Enables dynamic MAC registration of a user
group-name <GROUP-NAME>	Specifies the group to which the MAC registered user should be added • <GROUP-NAME> – Specify the group name.
expiry-time <1-1500>	Optional. Specifies the user expiry time in days from 1 - 1500
agreement-refresh <0-100>	Optional. Sets the time (in days), after which an inactive user has to refresh the WLAN's terms of agreement. For example, if the agreement refresh period is set to 10, a user logging in after 10 days of inactivity will be displayed the agreement page. and will be allowed WLAN access only after refreshing the terms of agreement. • <0-100> – Specify the number of days from 0 - 100.

Example

```
rfs7000-37FABE(config-wlan-1)#mac-registration group-name test expiry-time 100

rfs7000-37FABE(config-wlan-1)#mac-registration external host 172.16.10.8
proxy-mode through-controller
rfs7000-37FABE(config-wlan-1)#show context
wlan 1
 ssid 1
 bridging-mode tunnel
 encryption-type none
 authentication-type mac
 mac-registration group-name test expiry-time 100
```

```
 mac-registration external host 172.16.10.8 proxy-mode through-controller
rfs7000-37FABE(config-wlan-1)#

rfs4000-229D58(config-wlan-wlan-testing)#mac-registration group-name Group3 ?
  agreement-refresh  Specify when the agreement page should be displayed to
                     the user (in days)
  expiry-time        Specify the user expiry time in days
  <cr>
rfs4000-229D58(config-wlan-wlan-testing)#

rfs4000-229D58(config-wlan-wlan-testing)#mac-registration group-name Group3
agreement-refresh ?
  <0-100>  Agreement page will be displayed to the user if the user has not
           visited in the past (number of days)

rfs4000-229D58(config-wlan-wlan-testing)#

rfs4000-229D58(config-wlan-wlan-testing)#mac-registration group-name Group3
agreement-refresh 19
```

motorola-extensions

wlan-mode commands

Enables support for Motorola Solutions specific extensions to 802.11

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
motorola-extensions [move-command|smart-scan|symbol-load-information|
          wmm-load-information]
```

Parameters

```
motorola-extensions [move-command|smart-scan|symbol-load-information|
wmm-load-information]
```

motorola-extensions	Enables support for Brocade specific extensions to 802.11
move-command	Enables support for Brocade move (fast roaming) feature
smart-scan	Enables support for smart scanning feature
symbol-load-information	Enables support for the Symbol Technologies load information element (Element ID 173)
wmm-load-information	Enables support for the Brocade WMM load information element

Example

```
rfs7000-37FABE(config-wlan-test)#motorola-extensions wmm-load-information

rfs7000-37FABE(config-wlan-test)#show context
wlan test
 description TestWLAN
```

```
 ssid test
 bridging-mode local
 encryption-type tkip-ccmp
 authentication-type eap
 kerberos server timeout 12
 kerberos server primary host 172.16.10.2
 accounting syslog host 172.16.10.4 port 2
 data-rates 2.4GHz gn
 motorola-extensions wmm-load-information
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 captive-portal-enforcement fall-back
 ip dhcp trust
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 enforce-dhcp
 broadcast-dhcp validate-offer
 http-analyze controller
rfs7000-37FABE(config-wlan-test)#
```

no

wlan-mode commands

Negates WLAN mode commands and reverts values to their default

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no <PARAMETER>
```

Parameters

None

Usage Guidelines:

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
rfs7000-37FABE(config-wlan-test)#no ?
  accounting                          Configure how accounting records are
                                      created for this wlan
  acl                                 Actions taken based on ACL
                                      configuration [ packet drop being one
                                      of them]
  answer-broadcast-probes             Do not Include this wlan when
                                      responding to probe requests that do
                                      not specify an SSID
  association-list                    Configure the association list for
                                      the wlan
```

authentication-type	Reset the authentication to use on this wlan to default (none/Pre-shared keys)
broadcast-dhcp	Configure broadcast DHCP packet handling
broadcast-ssid	Do not advertise the SSID of the WLAN in beacons
captive-portal-enforcement	Configure how captive-portal is enforced on the wlan
client-access	Disallow client access on this wlan (no data operations)
client-client-communication	Disallow switching of frames from one wireless client to another on this wlan
client-load-balancing	Disable load-balancing of clients on this wlan
controller-assisted-mobility	Disable configure assisted mobility
data-rates	Reset data rate configuration to default
description	Reset the description of the wlan
downstream-group-addressed-forwarding	Disable downstream group addressed forwarding of packets
eap-types	Allow all EAP types on this wlan
encryption-type	Reset the encryption to use on this wlan to default (none)
enforce-dhcp	Drop packets from Wireless Clients with static IP address
fast-bss-transition	Disable support for 802.11r Fast BSS Transition
http-analyze	Enable HTTP URL analysis on the wlan
ip	Internet Protocol (IP)
kerberos	Configure kerberos authentication parameters
mac-authentication	Configure mac-authentication related parameters
mac-registration	Dynamic MAC registration of user
motorola-extensions	Disable support for Motorola-Specific extensions to 802.11
protected-mgmt-frames	Disable support for Protected Management Frames (IEEE 802.11w)
proxy-arp-mode	Configure handling of ARP requests with proxy-arp is enabled
radio-resource-measurement	Disable support for 802.11k Radio Resource Measurement
radius	Configure RADIUS related parameters
relay-agent	Configure dhcp relay agent info
shutdown	Enable the use of this wlan
ssid	Configure ssid
time-based-access	Reset time-based-access parameters to default
use	Set setting to use
vlan	Map the default vlan (vlan-id 1) to the wlan
vlan-pool-member	Delete a mapped vlan from this wlan
wep128	Reset WEP128 parameters
wep64	Reset WEP64 parameters
wireless-client	Configure wireless-client specific parameters
wpa-wpa2	Modify tkip-ccmp (wpa/wpa2) related parameters

```
  service                                  Service to monitor to show no-service
                                           page to user

rfs7000-37FABE(config-wlan-test)#

The test settings before execution of the no command:

rfs7000-37FABE(config-wlan-test)#show context
wlan test
 description TestWLAN
 ssid test
 bridging-mode local
 encryption-type tkip-ccmp
 authentication-type eap
 kerberos server timeout 12
 kerberos server primary host 172.16.10.2
 accounting syslog host 172.16.10.4 port 2
 data-rates 2.4GHz gn
 motorola-extensions wmm-load-information
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 captive-portal-enforcement fall-back
 ip dhcp trust
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 enforce-dhcp
 broadcast-dhcp validate-offer
 http-analyze controller
rfs7000-37FABE(config-wlan-test)#

rfs7000-37FABE(config-wlan-test)#no accounting syslog

rfs7000-37FABE(config-wlan-test)#no description

rfs7000-37FABE(config-wlan-test)#no authentication-type

rfs7000-37FABE(config-wlan-test)#no encryption-type

rfs7000-37FABE(config-wlan-test)#no enforce-dhcp

rfs7000-37FABE(config-wlan-test)#no kerberos server primary host

rfs7000-37FABE(config-wlan-test)#no kerberos server timeout

rfs7000-37FABE(config-wlan-test)#no data-rates 2.4GHz

rfs7000-37FABE(config-wlan-test)#no ip dhcp trust

rfs7000-37FABE(config-wlan-test)#no captive-portal-enforcement

The test settings after the execution of the no command:

rfs7000-37FABE(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type none
 motorola-extensions wmm-load-information
 client-load-balancing probe-req-intvl 5ghz 5
```

```
 client-load-balancing band-discovery-intvl 2
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 broadcast-dhcp validate-offer
 http-analyze controller
rfs7000-37FABE(config-wlan-test)#
```

proxy-arp-mode

wlan-mode commands

Enables proxy ARP mode for handling ARP requests

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
proxy-arp-mode [dynamic|strict]
```

Parameters

```
proxy-arp-mode [dynamic|strict]
```

proxy-arp-mode	Enables proxy ARP mode for handling ARP requests. The options available are dynamic and strict.
dynamic	Forwards ARP requests to the wireless side (for which a response could not be proxied)
strict	Does not forward ARP requests to the wireless side

Example

```
rfs7000-37FABE(config-wlan-test)#proxy-arp-mode strict

rfs7000-37FABE(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type none
 protected-mgmt-frames mandatory
 motorola-extensions wmm-load-information
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 proxy-arp-mode strict
 broadcast-dhcp validate-offer
 http-analyze controller
rfs7000-37FABE(config-wlan-test)#
```

radio-resource-measurement

wlan-mode commands

Enables support for 802.11k radio resource measurement

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
radio-resource-measurement {channel-report}
```

Parameters

```
radio-resource-measurement {channel-report}
```

radio-resource-measurement {channel-report}	Enables support for 802.11k radio resource measurement • channel-report – Optional. Includes the channel-report element in beacons and probe responses

Example

```
rfs4000-229D58(config-wlan-test)#radio-resource-measurement
rfs4000-229D58(config-wlan-test)#

rfs4000-229D58(config-wlan-test)#show context
wlan test
 ssid test
 vlan 1
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 radio-resource-measurement
 controller-assisted-mobility
rfs4000-229D58(config-wlan-test)#
```

radius

wlan-mode commands

Configures RADIUS related parameters

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
radius [dynamic-authorization|nas-identifier|nas-port-id|vlan-assignment]

radius [dynamic-authorization|nas-identifier <NAS-ID>|nas-port-id
<NAS-PORT-ID>|
          vlan-assignment]
```

Parameters

```
radius [dynamic-authorization|nas-identifier <NAS-ID>|nas-port-id
<NAS-PORT-ID>|
vlan-assignment]
```

dynamic-authorization	Enables support for disconnect and change of authorization messages (RFC5176)
nas-identifier <NAS-ID>	Configures the WLAN NAS identifier sent to the RADIUS server. The NAS identifier should not exceed 256 characters.
nas-port-id <NAS-PORT-ID>	Configures the WLAN NAS port ID sent to the RADIUS server. The NAS port identifier should not exceed 256 characters.
vlan-assignment	Configures the VLAN assignment of a WLAN When enabled, this option assigns clients to the RADIUS server specified VLANs. This option is disabled by default.

Example

```
rfs7000-37FABE(config-wlan-test)#radius vlan-assignment

rfs7000-37FABE(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type none
 protected-mgmt-frames mandatory
 radius vlan-assignment
 motorola-extensions wmm-load-information
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 proxy-arp-mode strict
 broadcast-dhcp validate-offer
 http-analyze controller
rfs7000-37FABE(config-wlan-test)#
```

relay-agent

wlan-mode commands

Enables support for DHCP relay agent information (option 82) feature on this WLAN

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
relay-agent dhcp-option82
```

Parameters

```
relay-agent dhcp-option82
```

relay-agent dhcp-option82	Supports DHCP option 82. When enabled, this feature allows the DHCP relay agent to insert the relay agent information option (option 82) in client requests forwarded to the DHCP server. This information provides the following: • circuit ID suboption – Provides the SNMP port interface index • remote ID – Provides the controller's MAC address

Example

```
rfs4000-229D58(config-wlan-test)#relay-agent dhcp-option82
rfs4000-229D58(config-wlan-test)#

rfs4000-229D58(config-wlan-test)#show context
wlan test
 ssid test
 vlan 1
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 radio-resource-measurement
 relay-agent dhcp-option82
 controller-assisted-mobility
rfs4000-229D58(config-wlan-test)#
```

shutdown

wlan-mode commands

Shuts down a WLAN

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
shutdown {on-critical-resource|on-meshpoint-loss|on-primary-port-link-loss|
          on-unadoption}
```

Parameters

```
shutdown {on-critical-resource|on-meshpoint-loss|on-primary-port-link-loss|
on-unadoption}
```

shutdown	Shuts down the WLAN when specified events occur. Disabled by default.
on-critical-resource	Optional. Shuts down the WLAN when critical resource failure occurs. Disabled by default.
on-meshpoint-loss	Optional. Shuts down the WLAN when the root meshpoint link fails (is unreachable). Disabled by default.
on-primary-port-link-loss	Optional. Shuts down the WLAN when a device losses its primary Ethernet port (ge1/up1) link. Disabled by default.
on-unadoption	Optional. Shuts down the WLAN when an adopted device becomes unadopted. Disabled by default.

Usage Guidelines:

If the shutdown on-meshpoint-loss feature is enabled, the WLAN status changes only if the meshpoint and the WLAN are mapped to the same VLAN. If the meshpoint is mapped to VLAN 1 and the WLAN is mapped to VLAN 2, then the WLAN status does not change on loss of the meshpoint.

Example

```
rfs7000-37FABE(config-wlan-test)#shutdown on-unadoption

rfs7000-37FABE(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type none
 protected-mgmt-frames mandatory
 radius vlan-assignment
 motorola-extensions wmm-load-information
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 proxy-arp-mode strict
 broadcast-dhcp validate-offer
 shutdown on-unadoption
 http-analyze controller
rfs7000-37FABE(config-wlan-test)#
```

ssid

wlan-mode commands

Configures a WLAN's SSID

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
ssid <SSID>
```

Parameters

```
ssid <SSID>
```

<SSID>	Specify the WLAN's SSID. The WLAN SSID is case sensitive and alphanumeric. Its length should not exceed 32 characters.

Example

```
rfs7000-37FABE(config-wlan-test)#ssid testWLAN1

rfs7000-37FABE(config-wlan-test)#show context
wlan test
 ssid testWLAN1
 bridging-mode local
```

```
 encryption-type none
 authentication-type none
 protected-mgmt-frames mandatory
 radius vlan-assignment
 motorola-extensions wmm-load-information
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 proxy-arp-mode strict
 broadcast-dhcp validate-offer
 shutdown on-unadoption
 http-analyze controller
rfs7000-37FABE(config-wlan-test)#
```

time-based-access

wlan-mode commands

Configures time-based client access to the network resources

Administrators can use this feature to assign fixed days and time of WLAN access for wireless clients

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
time-based-access days [sunday|monday|tuesday|wednesday|thursday|friday|
          saturday|all|weekends|weekdays] {start <START-TIME>} [end
<END-TIME>]
```

Parameters

```
time-based-access days [sunday|monday|tuesday|wednesday|thursday|friday|
saturday|all|weekends|weekdays] {start <START-TIME>} [end <END-TIME>]
```

day <option>	Specifies the day or days on which the client can access the WLAN • sunday – Allows access on Sundays only • monday – Allows access on Mondays only • Tuesday – Allows access on Tuesdays only • wednesday – Allows access on Wednesdays only • thursday – Allows access on Thursdays only • friday – Allows access on Fridays only • saturday – Allows access on Saturdays only • weekends – Allows access on weekends only • weekdays – Allows access on weekdays only • all – Allows access on all days
start <START-TIME>	Optional. Specifies the access start time in hours and minutes (HH:MM)
end <END-TIME>	Specifies the access end time in hours and minutes (HH:MM)

Usage Guidelines:

Ensure the system clock is configured correctly.

Example

```
rfs7000-37FABE(config-wlan-test)#time-based-access days weekdays start 10:00
end
 16:30

rfs7000-37FABE(config-wlan-test)#show context
wlan test
 ssid testWLAN1
 bridging-mode local
 encryption-type none
 authentication-type none
 protected-mgmt-frames mandatory
 radius vlan-assignment
 time-based-access days weekdays start 10:00 end 16:30
 motorola-extensions wmm-load-information
 client-load-balancing probe-req-intvl 5ghz 5
 --More--
rfs7000-37FABE(config-wlan-test)#
```

use

wlan-mode commands

This command associates an existing captive portal with a WLAN.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
use
[aaa-policy|association-acl-policy|captive-portal|ip-access-list|mac-access-l
ist|
          passpoint-policy|wlan-qos-policy]

use [aaa-policy <AAA-POLICY-NAME>|association-acl-policy
<ASSOCIATION-POLICY-NAME>|
          captive-portal <CAPTIVE-PORTAL-NAME>|passpoint-policy
<PASSPOINT-POLICY-NAME>|
          wlan-qos-policy <WLAN-QOS-POLICY-NAME>]

use ip-access-list [in|out] <IP-ACCESS-LIST-NAME>

use mac-access-list [in|out] <MAC-ACCESS-LIST-NAME>
```

Parameters

	`use [aaa-policy <AAA-POLICY-NAME>|association-acl-policy <ASSOCIATION-POLICY-NAME>| captive-portal <CAPTIVE-PORTAL-NAME>|passpoint-policy <PASSPOINT-POLICY-NAME>| wlan-qos-policy <WLAN-QoS-POLICY-NAME>]`
aaa-policy <AAA-POLICY-NAME>	Uses an existing AAA policy with a WLAN • <AAA-POLICY-NAME> – Specify the AAA policy name.
association-acl <ASSOCIATION-POLICY-NAME>	Uses an existing association ACL policy with a WLAN • <ASSOCIATION-POLICY-NAME> – Specify the association ACL policy name.
captive-portal <CAPTIVE-PORTAL-NAME>	Enables a WLAN's captive portal authentication • <CAPTIVE-PORTAL-NAME> – Specify the captive portal name.
passpoint-policy <PASSPOINT-POLICY-NAME>	Associates a passpoint policy (Hotspot2 configuration) with this WLAN. • <PASSPOINT-POLICY-NAME> – Specify the Hotspot 2.0 policy name. For more information on passpoint policy, see *PASSPOINT POLICY*. Map a passpoint policy to a WLAN. Since the configuration gets applied to the radio by BSS, only the Hotspot 2.0 configuration of primary WLANs on a BSSID is used. Incoming Hotspot 2.0 GAQ/ANQP requests from clients are identified by their destination MAC addresses and are handled by the passpoint policy from the primary WLAN on that BSS. Define one passpoint policy for every WLAN configured.
wlan-qos-policy <WLAN-QOS-POLICY-NAME>	Uses an existing WLAN QoS policy with a WLAN • <wlan-qos-policy-name> – Specify the WLAN QoS policy name.
	`use ip-access-list [in|out] <IP-ACCESS-LIST-NAME>`
ip-access-list [in|out] <IP-ACCESS-LIST-NAME>	Specifies the IP access list for incoming and outgoing packets • in – Incoming packets • out – Outgoing packets • <IP-ACCESS-LIST-NAME> – Specify the IP access list name.
	`use mac-access-list [in|out] <MAC-ACCESS-LIST-NAME>`
mac-access-list [in|out] <MAC-ACCESS-LIST-NAME>	Specifies the MAC access list for incoming and outgoing packets. • in – Incoming packets • out – Outgoing packets • <MAC-ACCESS-LIST-NAME> – Specify the MAC access list name.

Usage Guidelines:

IP and MAC ACLs act as firewalls within a WLAN. WLANs use ACLs as firewalls to filter or mark packets based on the WLAN from which they arrive, as opposed to filtering packets on layer 2 ports. An ACL contains an ordered list of *Access Control Entries* (ACEs). Each ACE specifies a set of conditions (rules) and the action taken in case of a match. The action can be permit, deny, or mark. Therefore, when a packet matches an ACE's conditions, it is either forwarded, dropped, or marked depending on the action specified in the ACE. The order of conditions in the list is critical since filtering is stopped after the first match.

IP ACLs contain deny and permit rules specifying source and destination IP addresses. Each rule has a precedence order assigned. Both IP and non-IP traffic on the same layer 2 interface can be filtered by applying both an IP ACL and a MAC.

Additionally, you can filter layer 2 traffic on a physical layer 2 interface using MAC addresses. A MAC firewall rule uses source and destination MAC addresses for matching operations, where the result is a typical allow, deny, or mark designation to WLAN packet traffic.

Keep in mind IP and non-IP traffic on the same layer 2 interface can be filtered by applying both an IP ACL and a MAC ACL to the interface.

Example

```
rfs7000-37FABE(config-wlan-test)#use aaa-policy test

rfs7000-37FABE(config-wlan-test)#use association-acl-policy test

rfs7000-37FABE(config-wlan-test)#show context
wlan test
 ssid testWLAN1
 bridging-mode local
 encryption-type none
 authentication-type none
 protected-mgmt-frames mandatory
 radius vlan-assignment
 time-based-access days weekdays start 10:00 end 16:30
 motorola-extensions wmm-load-information
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 use aaa-policy test
 use association-acl-policy test
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 proxy-arp-mode strict
 broadcast-dhcp validate-offer
 shutdown on-unadoption
 http-analyze controller
rfs7000-37FABE(config-wlan-test)#
```

vlan

wlan-mode commands

Sets the VLAN where traffic from a WLAN is mapped

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
vlan [<1-4094>|<VLAN-ALIAS-NAME>]
```

Parameters

```
vlan [<1-4094>|<VLAN-ALIAS-NAME>]
```

<1-4094>	Sets a WLAN's VLAN ID. This command starts a new VLAN assignment for a WLAN index. All prior VLAN settings are erased. Use this command to assign just one VLAN to the WLAN. Utilizing a single VLAN per WLAN is a more typical deployment scenario than using a VLAN pool.
<VLAN-ALIAS-NAME>	Assigns a VLAN alias to the WLAN. The VLAN alias should to existing and configured. A VLAN alias maps a name to a VLAN ID. When applied to ports (for example GE ports) using the trunk mode, a VLAN alias denies or permits traffic, on the port, to and from the VLANs specified in the alias. For more information on aliases, see *alias*.

Example

```
rfs7000-37FABE(config-wlan-test)#vlan 4

rfs7000-37FABE(config-wlan-test)#show context
wlan test
 ssid testWLAN1
 vlan 4
 bridging-mode local
 encryption-type none
 authentication-type none
 protected-mgmt-frames mandatory
 radius vlan-assignment
 time-based-access days weekdays start 10:00 end 16:30
 motorola-extensions wmm-load-information
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 use aaa-policy test
 use association-acl-policy test
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 proxy-arp-mode strict
 broadcast-dhcp validate-offer
 shutdown on-unadoption
 http-analyze controller
rfs7000-37FABE(config-wlan-test)#
```

vlan-pool-member

wlan-mode commands

Adds a member VLAN to a WLAN's VLAN pool

NOTE
Configuration of a VLAN pool overrides the 'vlan' configuration.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
vlan-pool-member <WORD> {limit <0-8192>}
```

Parameters

```
vlan-pool-member <WORD> {limit <0-8192>}
```

vlan-pool-member	Adds a member VLAN to a WLAN's VLAN pool
<WORD>	Define the VLANs available to this WLAN. It is either a single index, or a list of VLAN IDs (for example, 1,3,7), or a range (for example, 1-10)
limit <0-8192>	Optional. Is ignored if the number of clients are limited and well within the limits of the DHCP pool on the VLAN • <0-8192> – Specifies the number of users allowed

Example

```
rfs7000-37FABE(config-wlan-test)#vlan-pool-member 1-10 limit 1

rfs7000-37FABE(config-wlan-test)#show context
wlan test
 ssid testWLAN1
 vlan-pool-member 1 limit 1
 vlan-pool-member 2 limit 1
 vlan-pool-member 3 limit 1
 vlan-pool-member 4 limit 1
 vlan-pool-member 5 limit 1
 vlan-pool-member 6 limit 1
 vlan-pool-member 7 limit 1
 vlan-pool-member 8 limit 1
 vlan-pool-member 9 limit 1
 vlan-pool-member 10 limit 1
 bridging-mode local
 encryption-type none
 authentication-type none
 protected-mgmt-frames mandatory
 radius vlan-assignment
 time-based-access days weekdays start 10:00 end 16:30
 motorola-extensions wmm-load-information
 --More--
rfs7000-37FABE(config-wlan-test)#
```

wep128

wlan-mode commands

Configures WEP128 parameters

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
wep128 [key|keys-from-passkey|transmit-key]

wep128 key <1-4> [ascii|hex] [0 <WORD>|2 <WORD>|<WORD>]
```

```
wep128 keys-from-passkey <WORD>

wep128 transmit-key <1-4>
```

Parameters

```
wep128 key <1-4> [ascii|hex] [0 <WORD>|2 <WORD>|<WORD>]
```

wep128	Configures WEP128 parameters. The parameters are: key, key-from-passkey, and transmit-key.
key <1-4>]	Configures pre-shared hex keys • <1-4> – Configures a maximum of four key indexes. Select the key index from 1 - 4.
ascii [0 <WORD>| 2 <WORD>|<WORD>]	Sets keys as ASCII characters (5 characters for WEP64, 13 for WEP128) • 0 <WORD> – Configures a clear text key • 2 <WORD> – Configures an encrypted key • <WORD> – Configures keys as 13 ASCII characters converted to hex, or 26 hexadecimal characters
hex [0 <WORD>| 2 <WORD>|<WORD>]	Sets keys as hexadecimal characters (10 characters for WEP64, 26 for WEP128) • 0 <WORD> – Configures a clear text key • 2 <WORD> – Configures an encrypted key • <WORD> – Configures keys as 13 ASCII characters converted to hex, or 26 hexadecimal characters

```
wep128 keys-from-passkey <WORD>
```

keys-from-passkey <WORD>	Specifies a passphrase from which keys are derived • <WORD> – Specify a passphrase from 4 - 32 characters.

```
wep128 transmit-key <1-4>
```

transmit-key <1-4>	Configures the key index used for transmission from an AP to a wireless client or service platform • <1-4> – Specify a key index from 1 - 4.

Example

```
rfs7000-37FABE(config-wlan-test)#wep128 keys-from-passkey
motorolasolutions@123

rfs7000-37FABE(config-wlan-test)#show context
wlan test
 ssid testWLAN1
 vlan-pool-member 1 limit 1
 vlan-pool-member 2 limit 1
 vlan-pool-member 3 limit 1
 vlan-pool-member 4 limit 1
 vlan-pool-member 5 limit 1
 vlan-pool-member 6 limit 1
 vlan-pool-member 7 limit 1
 vlan-pool-member 8 limit 1
 vlan-pool-member 9 limit 1
 vlan-pool-member 10 limit 1
 bridging-mode local
 encryption-type none
 authentication-type none
 protected-mgmt-frames mandatory
 wep128 key 1 hex 0 25f6e7ed9718918a87a75acc75
 wep128 key 2 hex 0 2b3fb36924b22dffe98c86c315
 wep128 key 3 hex 0 1ebf3394431700194762ebd5b2
 wep128 key 4 hex 0 e3de75be311bd787aeac5e4e8b
 radius vlan-assignment
 time-based-access days weekdays start 10:00 end 16:30
--More--
```

```
rfs7000-37FABE(config-wlan-test)#
```

wep64

wlan-mode commands

Configures WEP64 parameters

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
wep64 [key|keys-from-passkey|transmit-key]

wep64 key <1-4> [ascii|hex] [0 <WORD>|2 <WORD>|<WORD>]

wep64 keys-from-passkey <WORD>

wep64 transmit-key <1-4>
```

Parameters

```
wep64 key <1-4> [ascii|hex] [0 <WORD>|2 <WORD>|<WORD>]
```

wep64	Configures WEP64 parameters The parameters are: key, key-from-passkey, and transmit-key.
key <1-4>]	Configures pre-shared hex keys • <1-4> – Configures a maximum of four key indexes. Select a key index from 1 - 4.
ascii [0 <WORD>| 2 <WORD>|<WORD>]	Sets keys as ASCII characters (5 characters for WEP64, 13 for WEP128) • 0 <WORD> – Configures a clear text key • 2 <WORD> – Configures an encrypted key • <WORD> – Configures key (10 hex or 5 ASCII characters for WEP64, 26 hex or 13 ASCII characters for WEP128).
hex [0 <WORD>| 2 <WORD>|<WORD>]	Sets keys as hexadecimal characters (10 characters for WEP64, 26 for WEP128) • 0 <WORD> – Configures a clear text key • 2 <WORD> – Configures an encrypted key • <WORD> – Configures the key (10 hex or 5 ASCII characters for WEP64, 26 hex or 13 ASCII characters for WEP128)

```
wep64 keys-from-passkey <WORD>
```

keys-from-passkey <WORD>	Specifies a passphrase from which keys are derived • <WORD> – Specify a passphrase from 4 - 32 characters.

```
wep64 transmit-key <1-4>
```

transmit-key <1-4>	Configures the key index used for transmission from an AP to a wireless client or service platform • <1-4> – Specify a key index from 1 - 4.

Example

```
rfs7000-37FABE(config-wlan-test)#wep64 key 1 ascii motor

rfs7000-37FABE(config-wlan-test)#wep64 transmit-key 1

rfs7000-37FABE(config-wlan-test)#show context
wlan test
 ssid testWLAN1
 vlan-pool-member 1 limit 1
 vlan-pool-member 2 limit 1
 vlan-pool-member 3 limit 1
 vlan-pool-member 4 limit 1
 vlan-pool-member 5 limit 1
 vlan-pool-member 6 limit 1
 vlan-pool-member 7 limit 1
 vlan-pool-member 8 limit 1
 vlan-pool-member 9 limit 1
 vlan-pool-member 10 limit 1
 bridging-mode local
 encryption-type none
 authentication-type none
 protected-mgmt-frames mandatory
 wep64 key 1 hex 0 6d6f746f72
 radius vlan-assignment
 time-based-access days weekdays start 10:00 end 16:30
 motorola-extensions wmm-load-information
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 use aaa-policy test
--More--
rfs7000-37FABE(config-wlan-test)#
```

wireless-client

wlan-mode commands

Configures the transmit power indicated to clients

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
wireless-client
[count-per-radio|cred-cache-ageout|hold-time|inactivity-timeout|

max-firewall-sessions|reauthentication|roam-notification|tx-power|vlan-cache-
ageout]
```

```
wireless-client [count-per-radio <0-256>|cred-cache-ageout <60-86400>|
          hold-time <1-86400>|inactivity-timeout
<60-86400>|max-firewall-sessions <10-10000>|
          reauthentication <30-86400>|tx-power <0-20>|vlan-cache-ageout
<60-86400>]

wireless-client roam-notification [after-association|after-data-ready|auto]
```

Parameters

```
wireless-client [count-per-radio <0-256>|cred-cache-ageout <60-86400>|
hold-time <1-86400>|inactivity-timeout <60-86400>|max-firewall-sessions
<10-10000>|
reauthentication <30-86400>|tx-power <0-20>|vlan-cache-out <60-86400>]
```

wireless-client	Configures the transmit power indicated to wireless clients for transmission
count-per-radio <0-256>	Configures the maximum number of clients allowed on this WLAN per radio • <0-256> – Specify a value from 0 - 256.
cred-cache-ageout <60-86400>	Configures the timeout period for which client credentials are cached across associations • <60-86400> – Specify a value from 60 - 86400 seconds.
hold-time <1-86400>	Configures the time period for which wireless client state information is cached post roaming • <1-86400> – Specify a value from 1 - 86400 seconds.
inactivity-timeout <60-86400>	Configures an inactivity timeout period in seconds. If a frame is not received from a wireless client for this period of time, the client is disassociated. • <60-86400> – Specify a value from 60 - 86400 seconds.
max-firewall-sessions <10-10000>	Configures the maximum firewall sessions allowed per client on a WLAN • <10-10000> – Specify the maximum number of firewall sessions allowed from 10 - 10000.
reauthentication <30-86400>	Configures periodic reauthentication of associated clients • <30-86400> – Specify the client reauthentication interval from 30 - 86400 seconds.
tx-power <0-20>	Configures the transmit power indicated to clients • <0-20> – Specify a value from 0 - 20 dBm.
vlan-cache-ageout <60-86400>	Configures the timeout period for which client VLAN information is cached across associations. • <60-86400> – Specify a value from 60 - 86400 seconds.

```
wireless-client roam-notification [after-association|after-data-ready|auto]
```

wireless-client	Configures the transmit power indicated to wireless clients for transmission
roam-notification	Configures when a roam notification is transmitted
after-association	Transmits a roam notification after a client has associated
after-data-ready	Transmits a roam notification after a client is data-ready (after completion of authentication, handshakes etc.)
auto	Transmits a roam notification upon client association (if the client is known to have authenticated to the network)

Example

```
rfs7000-37FABE(config-wlan-test)#wireless-client cred-cache-ageout 65

rfs7000-37FABE(config-wlan-test)#wireless-client hold-time 200

rfs7000-37FABE(config-wlan-test)#wireless-client max-firewall-sessions 100
```

```
rfs7000-37FABE(config-wlan-test)#wireless-client reauthentication 35

rfs7000-37FABE(config-wlan-test)#wireless-client tx-power 12

rfs7000-37FABE(config-wlan-test)#show context
wlan test
 ssid testWLAN1
 vlan-pool-member 1 limit 1
 vlan-pool-member 2 limit 1
 vlan-pool-member 3 limit 1
 vlan-pool-member 4 limit 1
 vlan-pool-member 5 limit 1
 vlan-pool-member 6 limit 1
 vlan-pool-member 7 limit 1
 vlan-pool-member 8 limit 1
 vlan-pool-member 9 limit 1
 vlan-pool-member 10 limit 1
 bridging-mode local
 encryption-type none
 authentication-type none
 wireless-client hold-time 200
 wireless-client cred-cache-ageout 65
 wireless-client max-firewall-sessions 100
 protected-mgmt-frames mandatory
 wireless-client reauthentication 35
 wep64 key 1 hex 0 6d6f746f72
 wep128 key 1 hex 0 25f6e7ed9718918a87a75acc75
 wep128 key 2 hex 0 2b3fb36924b22dffe98c86c315
 wep128 key 3 hex 0 1ebf3394431700194762ebd5b2
 wep128 key 4 hex 0 e3de75be311bd787aeac5e4e8b
 radius vlan-assignment
 time-based-access days weekdays start 10:00 end 16:30
 motorola-extensions wmm-load-information
 wireless-client tx-power 12
 client-load-balancing probe-req-intvl 5ghz 5
--More--
rfs7000-37FABE(config-wlan-test)#
```

wpa-wpa2

wlan-mode commands

Modifies TKIP-CCMP (WPA/WPA2) related parameters

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
wpa-wpa2
[exclude-wpa2-tkip|handshake|key-rotation|opp-pmk-caching|pmk-caching|
          preauthentication|psk|tkip-countermeasures|use-sha256-akm]
```

```
wpa-wpa2 [exclude-wpa2-tkip|opp-pmk-caching|pmk-caching|preauthentication|
          use-sha256-akm]

wpa-wpa2 handshake [attempts|init-wait|priority|timeout]
wpa-wpa2 handshake [attempts <1-5>|init-wait <5-1000000>|priority
[high|normal]|
          timeout <10-5000> {10-5000}]

wpa-wpa2 key-rotation [broadcast|unicast] <30-86400>

wpa-wpa2 psk [0 <LINE>|2 <LINE>|<LINE>]

wpa-wpa2 tkip-countermeasures holdtime <0-65535>
```

Parameters

```
wpa-wpa2 [exclude-wpa2-tkip|opp-pmk-caching|pmk-caching|preauthentication|
use-sha256-akm]
```

wpa-wpa2	Modifies TKIP-CCMP (WPA/WPA2) related parameters
exclude-wpa2-tkip	Excludes the *Wi-Fi Protected Access II* (WPA2) version of TKIP. It supports the WPA version of TKIP only
opp-pmk-caching	Uses opportunistic key caching (same *Pairwise Master Key* (PMK) across APs for fast roaming with EAP.802.1x
pmk-caching	Uses cached pair-wise master keys (fast roaming with eap/802.1x)
preauthentication	Uses pre-authentication mode (WPA2 fast roaming)
use-sha256-akm	Uses sha256 authentication key management suite

```
wpa-wpa2 handshake [attempts <1-5>|init-wait <5-1000000>|priority
[high|normal]|
timeout <10-5000> {10-5000}]
```

wpa-wpa2	Modifies TKIP-CCMP (WPA/WPA2) related parameters
handshake	Configures WPA/WPA2 handshake parameters
attempts <1-5>	Configures the total number of times a message is transmitted towards a non-responsive client • <1-5> – Specify a value from 1 - 5.
init-wait <5-1000000>	Configures a minimum wait-time period, in microseconds, before the first handshake message is transmitted from the AP • <5-1000000> – Specify a value from 5 - 1000000 microseconds.
priority [high|normal]	Configures the relative priority of handshake messages compared to other data traffic • high – Treats handshake messages as high priority packets on a radio • normal – Treats handshake messages as normal priority packets on a radio
timeout <10-5000> <10-5000>	Configures the timeout period, in milliseconds, for a handshake message to retire. Once this period is exceed, the handshake message is retired. • <10-5000> – Specify a value from 10 - 5000 milliseconds. • <10-5000> – Optional. Configures a different timeout between the second and third attempts

```
wpa-wpa2 key-rotation [broadcast|unicast] <30-86400>
```

wpa-wpa2	Modifies TKIP-CCMP (WPA/WPA2) related parameters
key-rotation	Configures parameters related to periodic rotation of encryption keys. The periodic key rotation parameters are broadcast, multicast, and unicast traffic.

broadcast <30-86400>	Configures the periodic rotation of keys used for broadcast and multicast traffic. This parameter specifies the interval, in seconds, at which keys are rotated. • <30-86400> – Specify a value from 30 - 86400 seconds.
unicast <30-86400>	Configures a periodic interval for the rotation of keys, used for unicast traffic • <30-86400> – Specify a value from 30 - 86400 seconds.

```
wpa-wpa2 psk [0 <LINE>|2 <LINE>|<LINE>]
```

wpa-wpa2	Modifies TKIP-CCMP (WPA/WPA2) related parameters
psk	Configures a pre-shared key. The key options are: 0, 2, and LINE
0 <LINE>	Configures a clear text key
2 <LINE>	Configures an encrypted key
<LINE>	Enter the pre-shared key either as a passphrase not exceeding 8 - 63 characters, or as a 64 character (256bit) hexadecimal value

```
wpa-wpa2 tkip-countermeasures holdtime <0-65535>
```

wpa-wpa2	Modifies TKIP-CCMP (WPA/WPA2) parameters
tkip-countermeasures	Configures a hold time period for implementation of TKIP counter measures
holdtime <0-65535>	Configures the amount of time a WLAN is disabled when TKIP counter measures are invoked • <0-65535> – Specify a value from 0 - 65536 seconds.

Example

```
rfs7000-37FABE(config-wlan-test)#wpa-wpa2 tkip-countermeasures hold-time 2

rfs7000-37FABE(config-wlan-test)#show context
wlan test
 ssid testWLAN1
 vlan-pool-member 1 limit 1
 vlan-pool-member 2 limit 1
 vlan-pool-member 3 limit 1
 vlan-pool-member 4 limit 1
 vlan-pool-member 5 limit 1
 vlan-pool-member 6 limit 1
 vlan-pool-member 7 limit 1
 vlan-pool-member 8 limit 1
 vlan-pool-member 9 limit 1
 vlan-pool-member 10 limit 1
 bridging-mode local
 encryption-type none
 authentication-type none
 wireless-client hold-time 200
 wireless-client cred-cache-ageout 65
 wireless-client max-firewall-sessions 100
 protected-mgmt-frames mandatory
 wireless-client reauthentication 35
 wpa-wpa2 tkip-countermeasures hold-time 2
 wep64 key 1 hex 0 6d6f746f72
 wep128 key 1 hex 0 25f6e7ed9718918a87a75acc75
--More--
rfs7000-37FABE(config-wlan-test)#
```

service

wlan-mode commands

Invokes service commands applicable in the WLAN configuration mode

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
service
[allow-ht-only|allow-open-passpoint|cred-cache|eap-mac-mode|eap-mac-multicopy
|

eap-mac-multikeys|enforce-pmkid-validation|key-index|monitor|radio-crypto|

reauthentication|session-timeout|tx-deauth-on-roam-detection|unresponsive-cli
ent|
          show]

service [allow-ht-only|allow-open-passpoint|cred-cache clear-on-disconnect|

eap-mac-multicopy|eap-mac-multikeys|enforce-pmkid-validation|radio-crypto|
          reauthentication seamless|session-timeout
mac|tx-deauth-on-roam-detection|show cli]

service eap-mac-mode [mac-always|normal]

service key-index eap-wep-unicast <1-4>

service monitor [aaa-server|adoption vlan <1-4094>|captive-portal
external-server|
          dhcp crm <CRM-NAME> vlan <1-4094>]

service unresponsive-client [attempts <1-1000>|timeout <1-60>]
```

Parameters

```
service [allow-ht-only|allow-open-passpoint|cred-cache clear-on-disconnect|
eap-mac-multicopy|eap-mac-multikeys|enforce-pmkid-validation|radio-crypto|
reauthentication seamless|session-timeout
mac|tx-deauth-on-roam-detection|show cli]]
```

allow-ht-only	Only allows clients capable of High Throughput (802.11n) data rates to associate
allow-open-passpoint	Enables non-WPA2 security for passpoint WLANs. For more information on passpoint policy and configuration, see *PASSPOINT POLICY*.
cred-cache clear-on-disconnect	Clears credential cache after a client has disconnected from the network
eap-mac-multicopy	Enables sending of multiple copies of broadcast and unicast messages
eap-mac-multikeys	Enables configuration of different key indices for MAC authentication

enforce-pmkid-validation	Validates the *Predictive real-time pairwise master key identifier* (PMKID) contained in a client's association request against the one present in the wpa-wpa2 handshake This functionality is based on the *Proactive Key Caching* (PKC) extension of the 802.11i EEEE standard. Whenever a wireless client successfully authenticates with a AP it receives a *pairwise master key* (PMK). PKC allows clients to cache this PMK and reuse it for future re-authentications with the same AP. The PMK is unique for every client and is identified by the PMKID. The PMKID is a combination of the hash of the PMK, a string, the station and the MAC addresses of the AP.
radio-crypto	Uses radio hardware for encryption and decryption. This is applicable only for devices using *Counter Cipher Mode with Block Chaining Message Authentication Code Protocol* (CCMP) encryption mode.
reauthentication seamless	Enables seamless EAP client reauthentication without disconnecting client after the session has timed out
session-timeout mac	Enables reauthentication of MAC authenticated clients without disconnecting client after the session has timed out
tx-deauth-on-roam-detection	Transmits a deauthentication on the air while disassociating a client because its roam is detected on the wired side
show cli	Displays the CLI tree of the current mode. When used in the WLAN mode, this command displays the WLAN CLI structure.

```
service    eap-mac-mode [mac-always|normal]
```

eap-mac-mode	Configures the EAP and/or MAC authentication mode used with this WLAN
mac-always	Enables both EAP and MAC authentication. MAC authentication is performed first, followed by EAP authentication. Clients are granted access based on the EAP authentication result. If a client does not have EAP, the MAC authentication result is used to grant access.
normal	Grants client access if the client clears either EAP or MAC authentication

```
service key-index eap-wep-unicast <1-4>
```

key-index eap-wep-unicast <1-4>	Configures an index with each key during EAP authentication with WEP • <1-4> – Select a index form 1 - 4.

```
service monitor [aaa-server|adoption vlan <1-4094>|captive-portal
external-server|
dhcp crm <CRM-NAME> vlan <1-4094>]
```

monitor	Enables critical resources for failure
aaa-server‘	Enables AAA server failure monitoring. This feature is disabled by default.
adoption vlan <1-4094>	Enables adoption failure monitoring on an adopted AP. Also configures a adoption failover VLAN. This feature is disabled by default. • VLAN <1-4094> – Specify the VLAN on which clients are placed when the connectivity between the AAP and the controller is lost. Configure a DHCP pool and gateway for the failover VLAN. Ensure the DHCP server is running on the AP. Also ensure that the DHCP pool is configured to have less lease time. When this feature is enabled on a WLAN, it allows adopted APs to monitor their connectivity with the controller. If and when this connectivity is lost, all new clients are placed in the configured adoption failover VLAN. They are served an IP by the DHCP server running on the AP. In this situation if a client tries to access a Web URL, the AP redirects the client to a page stating that the service is down. When the AAP's link to the switch is restored, clients are placed back in the WLAN's configured VLAN, and are served an IP from the corresponding configured DHCP server (external or on the AP/controller).

captive-portal external-server	Enables external captive portal server failure monitoring. This feature is disabled by default. When enabled, this feature enables APs to display, to an externally located captive portal's user, the no-service page when the captive portal's server is not reachable.
dhcp crm <CRM-NAME> vlan <1-4094>	Enables external DHCP server failure monitoring. Also configures a DHCP failover VLAN. This feature is disabled by default. • crm <CRM-NAME> – Specified the names of the CRMs being monitored (i.e. the servers configured under this CRM are monitored). • VLAN <1-4094> – Specify the VLAN on which clients are placed when the connectivity between the AAP and the controller is lost. Configure a DHCP pool and gateway for the failover VLAN. Ensure the following: DHCP server is running on the AP, DHCP pool is configured to have less lease time, and the CRM for DHCP server to be monitored is configured on the AP. When this feature is enabled on a WLAN, it allows the monitoring of DHCP servers. If the DHCP server is unavailable, the AP disconnects all clients. These disconnected clients are placed in the specified CRM failover VLAN, and are served a new IP by the DHCP server running on the AP. In this situation if a client tries to access a Web URL, the AP redirects the client to a page stating that the service is down. Whenever there is a change in DHCP server availability, all associated clients are shifted back to the appropriate DHCP server and are served new IP addresses.

`service unresponsive-client [attempts <1-1000>|timeout <1-60>]`

eap-mac-mode	Configures handling of unresponsive clients
attempts <1-1000>	Configures the maximum number of successive packets that failed transmission • <1-1000> – Specify a value from 1 - 1000.
timeout <1-60>	Configures the interval, in seconds, for successive packets not acknowledged by the client • <1-60> – Specify a value from 1 - 60 seconds.

Example

```
rfs4000-229D58(config-wlan-test)#service allow-ht-only
rfs4000-229D58(config-wlan-test)#

rfs4000-229D58(config-wlan-test)#service monitor aaa-server
rfs4000-229D58(config-wlan-test)#

rfs4000-229D58(config-wlan-test)#show context
wlan test
 ssid test
 vlan 1
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 service monitor aaa-server
 service allow-ht-only
 controller-assisted-mobility
rfs4000-229D58(config-wlan-test)#
```

wlan-qos-policy

Global Configuration Commands

Configures a WLAN QoS policy

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
wlan-qos-policy <WLAN-QOS-POLICY-NAME>
```

Parameters

```
wlan-qos-policy <WLAN-QOS-POLICY-NAME>
```

<WLAN-QOS-POLICY-NAME>	Specify the WLAN QoS policy name. If the policy does not exist, it is created.

Example

```
rfs7000-37FABE(config)#wlan-qos-policy test
rfs7000-37FABE(config-wlan-qos-test)#?
WLAN QoS Mode commands:
  accelerated-multicast  Configure accelerated multicast streams address assnd
                         forwarding QoS classification
  classification         Select how traffic on this WLAN must be classified
                         (relative prioritization on the radio)
  multicast-mask         Egress multicast mask (frames that match bypass the
                         PSPqueue. This permits intercom mode operation
                         without delay even in the presence of PSP clients)
  no                     Negate a command or set its defaults
  qos                    Quality of service
  rate-limit             Configure traffic rate-limiting parameters on a
                         per-wlan/per-client basis
  svp-prioritization     Enable spectralink voice protocol support on this
                         wlan
  voice-prioritization   Prioritize voice client over other client (for
                         non-WMM clients)
  wmm                    Configure 802.11e/Wireless MultiMedia parameters

  clrscr                 Clears the display screen
  commit                 Commit all changes made in this session
  do                     Run commands from Exec mode
  end                    End current mode and change to EXEC mode
  exit                   End current mode and down to previous mode
  help                   Description of the interactive help system
  revert                 Revert changes
  service                Service Commands
  show                   Show running system information
  write                  Write running configuration to memory or terminal

rfs7000-37FABE(config-wlan-qos-test)#
```

NOTE
For more information on WLAN QoS policy commands, see *Chapter 22, WLAN-QOS-POLICY*.

Related Commands:

no	Removes an existing WLAN QoS Policy

smart-cache-policy

Global Configuration Commands

The following table lists the smart cache policy configuration commands.

Command	Description	Reference
smart-cache-policy	Creates a new smart cache policy and enters its configuration mode	page 371
smart-cache-policy-mode commands	Summarizes the smart cache policy configuration mode commands	page 372

smart-cache-policy

smart-cache-policy

Creates a new smart cache policy and enters its configuration mode

Content caching is a mechanism that allows temporary caching of frequently accessed content on intermediate network devices. When enabled, subsequent requests for the same content are serviced from the cache locally and not fetched from originating servers, resulting in reduced bandwidth usage, lower latency, and reduced data transfers from originating servers. The Mobility smart cache policy supports both forward caching and transparent caching.

Forward content caching stores content temporarily on the local network. This locally stored content can be retrieved, when required, without routing a request to an external server on the Internet.

Transparent content caching, on the other hand, acts as an intermediary for the originating servers and returns cached content to clients as if the data originated from the associated servers. Transparent caching proxies perform server load-balancing and compression to regulate load on the originating servers and reduce bandwidth usage.

The smart cache policy also supports dynamic content caching, allowing caching of content form popular video content sharing sites, such as youtube.com, cnn.com, msn.com etc.

Enabling content caching improves Web browsing (for data and video content) for consumers using Kiosks, tablets, and smart phones. A smart cache policy is enabled by associating it with a device or a profile.

Configure the policy's forward proxy, transparent proxy and several additional settings before actual HTML pages can be defined for the smart caching configuration.

Supported in the following platforms:

- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
smart-cache-policy <SMART-CACHE-POLICY-NAME>
```

Parameters

```
smart-cache-policy <SMART-CACHE-POLICY-NAME>
```

<SMART-CACHE-POLICY-NAME>	Creates a new smart content cache policy. Specify the policy name. If the policy does not exist, it is created.

Example

```
nx4500-5CFA2B(config)#smart-cache-policy ?
  SMART-CACHE-POLICY  Name of the content caching to be configured ( will be
                      created if it does not exist )

nx4500-5CFA2B(config)#smart-cache-policy test
nx4500-5CFA2B(config-smart-cache-policy-test)#

nx4500-5CFA2B(config-smart-cache-policy-test)#?
Content Cache Policy Mode commands:
  access-log          Log all client requests
  aging               Configure the refresh pattern
  cache               Configure cache management
  forward-proxy       Configure address and port for forward caching proxy
                      service
  http-access         Configure http filter
  no                  Negate a command or set its defaults
  parent-proxy        Configure parent proxy
  pre-fetch           Enable pre fetching of a URL list
  smart-cache         Content cache
  transparent-proxy   Transparent caching proxy

  clrscr              Clears the display screen
  commit              Commit all changes made in this session
  do                  Run commands from Exec mode
  end                 End current mode and change to EXEC mode
  exit                End current mode and down to previous mode
  help                Description of the interactive help system
  revert              Revert changes
  service             Service Commands
  show                Show running system information
  write               Write running configuration to memory or terminal

nx4500-5CFA2B(config-smart-cache-policy-test)#
```

smart-cache-policy-mode commands

smart-cache-policy

The following table summarises smart cache policy configuration commands.

Command	Description	Reference
access-log	Enables client request logging	page 373
aging	Configures the refresh pattern (aging parameters) for specific content types	page 373
cache	Configures cache management settings	page 375
forward-proxy	Configures the address and port for forward caching proxy service	page 376
http-access	Configures HTTP filters – *access control lists* (ACLs)	page 377
no	Removes or resets content cache policy settings	page 379
pre-fetch	Enables pre fetching of URL lists	page 380
parent-proxy	Enables/disables parent proxy on this smart cache policy	page 381
smart-cache	Enables smart content caching	page 381
transparent-proxy	Configures transparent caching proxy settings	page 382

access-log

smart-cache-policy-mode commands

Enables or disables client request logging. When enabled, this feature logs client access details to the */var/log/smart-cache.log*. This feature is enabled by default.

Supported in the following platforms:

- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
access-log {rotate <0-10> rotate-type [duration <1-100> day|size <1-100> MB]}
```

Parameters

```
access-log {rotate <0-10> rotate-type [duration <1-100> day|size <1-100> MB]}
```

rotate <0-10>	Optional. Enables log file rotation, and configures the number of rotation. This is the number of log files retained (stored locally) out of the total generated. • <0-10> – Optional. Specify the number of rotations from 0 - 10. The default is 10 rotations on every 1 MB.
rotate-type [duration <1-100> day| size <1-100> MB]	Optional. Configures access log file rotation conditions, such as duration and size • duration <1-100> – Rotates log files by time. Specify the time from 1 - 100 days. The default is 1 day. • size <1-100> – Rotates log files by file size. Specify the size from 1 - 100 MB.

Example

```
nx4500-5CFA2B(config-smart-cache-policy-test)#access-log rotate 10
rotate-type duration 10 day
nx4500-5CFA2B(config-smart-cache-policy-test)#

nx4500-5CFA2B(config-smart-cache-policy-test)#show context
smart-cache-policy test
 access-log rotate 10 rotate-type duration 10 day
nx4500-5CFA2B(config-smart-cache-policy-test)#
```

Related Commands:

no	Disables client request logging

aging

smart-cache-policy-mode commands

Configures the aging rule (refresh pattern) for specific content types

The aging parameters configured are the maximum and minimum age, freshness factor, and the URL regular expressions. These parameters enable the content caching engine to determine if a given request can be processed and the content loaded from the cache or not.

Supported in the following platforms:

- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
aging precedence <1-100> [<WORD>|ignore-case <WORD>] min-age <0-525600>
          freshness-factor <0-100> max-age <0-525600>
{(override-expire|override-lastmod|
          reload-into-ims)}
```

Parameters

```
aging precedence <1-100> [<WORD>|ignore-case <WORD>] min-age <0-525600>
freshness-factor <0-100> max-age <0-525600>
{(override-expire|override-lastmod|
reload-into-ims)}
```

aging precedence <1-100>	Configures content cache aging rules and assigns a precedence to each rule • precedence <1-100> – Specify a precedence for this aging rule.
<WORD>	Specifies the regular expression to match. This option is case sensitive, and is the default setting.
ignore-case <WORD>	Specifies the regular expression to match. This option is not case sensitive.
min-age <0-525600>	Configures the minimum age, in minutes, of matched objects. This value specifies the lower limit on the staleness of a response. A response is not considered stale unless its time in the cache exceeds the specified minimum value. • <0-525600> – Specify a value from 0 - 525600 minutes. The default is 1 minute.
freshness-factor <0-100>	Configures the freshness factor of matched objects as a percentage value. Freshness is an expression of how long Web content resides on the service platform's local cache before being updated or removed. • <0-100> – Specify a value from 0 - 100%. The default is 100%.
max-age <0-525600>	Configures the maximum age, in minutes, of matched objects. This value specifies the upper limit on the freshness of a response. A response is not considered fresh unless its time in the cache is less than the specified maximum value. • <0-525600> – Specify a value from 0 - 525600 minutes. The default is 525600.
(override-expire| override-lastmod| |reload-into-ims)	Applies overrides. The options are: • override-expire – Optional. When selected, this option overrides the server sent explicit expiry time by the configured minimum age value. This option causes the content cache engine to check the min value before checking the Expires header. Thus, a non-zero min time makes the engine return an un-validated cache hit even if the response is pre-expired. • override-lastmod – Optional. When selected, this option enforces minimum age even on objects that were modified recently to force the minimum age period on recently modified cached content. This option causes the content cache engine to check the min value before the LM-factor percentage. • reload-into-ims – Optional. When selected, this option makes the content cache engine to transform a request with a no-cache directive into a validation (If-Modified-Since) request. In other words, the engine adds an If-Modified-Since header to the request before forwarding. Note: This works only for objects that have a Last-Modified timestamp. The outbound request retains the *nocache* directive, so that it reaches the originating server.

Example

```
nx4500-5CFA2B(config-smart-cache-policy-test)#aging precedence 1 ignore-case
\\.jgp$ min-age 100 freshness-factor 75 max-age 200 reload-into-ims
nx4500-5CFA2B(config-smart-cache-policy-test)#

nx4500-5CFA2B(config-smart-cache-policy-test)#show context
smart-cache-policy test
 aging precedence 1 ignore-case \\.jgp$ min-age 100 freshness-factor 75
max-age 200 reload-into-ims
 access-log rotate 10 rotate-type duration 10 day
nx4500-5CFA2B(config-smart-cache-policy-test)#
```

Related Commands:

no	Removes an existing aging rule (refresh pattern)

cache

smart-cache-policy-mode commands

Configures cache management settings

This command specifies content cache rules that determine if a content is cached or not. Use this feature to filter content before caching. By default content is not cached.

Supported in the following platforms:

- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
cache [media|precedence|size]

cache media {(all|aol|bing|break|cnn|daily-motion|metacafe|vimeo|youtube)}

cache precedence <1-100> [deny|permit] {destination-domain <DOMAIN-NAME>|
          destination-domain-regex <WORD>|destination-ip
[<IP>/M|any]|source-ip <IP>|
          url-regex <URL>}

cache size <1-32>
```

Parameters

```
cache media {(all|aol|bing|break|cnn|daily-motion|metacafe|vimeo|youtube)}
```

cache media	Enables content caching from the following video content sharing sites. The sites currently supported are: • aol.com • bing.com • break.com • dailymotion.com • metacafe.com • vimeo.com • cnn.com • youtube.com Select *All* to include the entire list of supported sites. Selected sites have their video content cached locally on the service platform and made available to clients that request the video content.

```
cache precedence <1-100> [deny|permit] {destination-domain <DOMAIN-NAME>|
destination-domain-regex <WORD>|destination-ip [<IP>/M|any]|source-ip
<IP>|url-regex <URL>}
```

cache precedence <1-100>	Configures cache filtering rules that determine if a content received from the originating server is to be cached or not. You can create multiple cache filtering rules and assign precedence values to each. These rules are applied in order of their precedence. • <1-100> – Specify a precedence rule from 1 - 100.
[deny|permit]	Configures the deny or permit caching parameters for this rule • permits – Caches content if it matches the defined permit parameters • deny – Does not cache content if it matches the defined deny parameters

destination-domain <DOMAIN-NAME>	Optional. Specifies the destination domain's hostname to match. The domain name can be an FQDN. The specified value is matched against the hostname part of the HTTP request URL. A leading asterisk or period in the domain name is treated as a wild card. For example, *www.brocade.com*, *brocade.com*, **.brocade.com* and *.com* are all valid values. The destination domain parameter will NOT match against URLs that have an IP address instead of a hostname.
destination-domain-regex <WORD>	Optional. Specifies a regular expression matching on originating server names The destination domain regex is the same as the destination domain, but the destination domain regex allows your to use standard expression matching on originating server names.
destination-ip [<IP>/M|any]	Optional. Specifies the originating server's IP address, obtained from the HTTP request URL Provide the IP address in the A.B.C.D/M format. Specify *any* to consider all originating servers.
source-ip [<IP>/M|any]	Optional. Specifies the source IP address (client's IP address) that is sent out as part of the HTTP request. Provide the IP address in the A.B.C.D/M format. Specify *any* to consider all client requests.
url-regex <URL>	Optional. Specifies regular expressions used to match any part of a requested URL, including the transfer protocol and origin server hostname

```
cache size <1-32>
```

cache size <1-32>	Configures the maximum caching storage size. This is upper limit on the disk space used for storing cached contents. • <1-32 > – Specify a value from 1 - 32 GB. The default is 32 GB.

Example

```
nx4500-5CFA2B(config-smart-cache-policy-test)#cache size 30
nx4500-5CFA2B(config-smart-cache-policy-test)#

nx4500-5CFA2B(config-smart-cache-policy-test)#show context
smart-cache-policy test
 cache size 30
 aging precedence 1 ignore-case \\.jgp$ min-age 100 freshness-factor 75
max-age 200 reload-into-ims
 access-log rotate 10 rotate-type duration 10 day
nx4500-5CFA2B(config-smart-cache-policy-test)#
```

Related Commands:

no	Resets or removes cache management settings

forward-proxy

smart-cache-policy-mode commands

Enables or disables forward proxy mode on this smart cache policy. This option is disabled by default.

Devices using this smart-cache policy act as a forward proxy on specified VLANs.

This command configures the IP address and port on which the forward proxy server listens for incoming HTTP requests.

Forward content caching stores content temporarily on the local network. This locally stored content can be retrieved, when required, without routing a request to an external server on the Internet.

Supported in the following platforms:

- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
forward-proxy {ip|protocol|vlan}

forward-proxy {ip <IP> port <1-32768>}

forward-proxy {protocol [all|ftp|gopher|https]}

forward-proxy {vlan <VLAN-ID>}
```

Parameters

```
forward-proxy (ip <IP> port <1-32768>}
```

ip <IP> port <1-32768>	Optional. Configures the IP address and TCP port for forward proxying This is the IP address where the forward smart caching proxy server is listening. The default port is 1.

```
forward-proxy {protocol [all|ftp|gopher|https]}
```

protocol [all|ftp|gropher|https]	Optional. Selects the additional forward proxy resource protocol for smart caching. the options are: • ftp – Selects FTP as the forward proxy resource protocol • gopher – Selects Gopher as the forward proxy resource protocol • https – Selects HTTPS as the forward proxy resource protocol • all – Selects all protocols

```
forward-proxy {vlan <VLAN-ID>}
```

vlan <VLAN-ID>	Optional. Configures the VLAN(s) for which forward proxy mode (content caching) is enabled. By default content caching is disabled on all VLANs. • <VLAN-ID> – Specify the list of VLANs.

Example

```
nx4500-5CFA2B(config-smart-cache-policy-test)#forward-proxy vlan 10-20
nx4500-5CFA2B(config-smart-cache-policy-test)#

nx4500-5CFA2B(config-smart-cache-policy-test)#show context
smart-cache-policy test
 forward-proxy vlan 10-20
 cache size 30
 aging precedence 1 ignore-case \\.jgp$ min-age 100 freshness-factor 75
max-age 200 reload-into-ims
 access-log rotate 10 rotate-type duration 10 day
nx4500-5CFA2B(config-smart-cache-policy-test)#
```

Related Commands:

no	Reverts address and port for forward caching proxy service

http-access

smart-cache-policy-mode commands

4

Configures HTTP filters. This command configures rules to deny or permit HTTP access. A deny rule specifies the destination domains and source and destination IPs to deny content access. A permit rule specifies the destination domains and source and destination IPs to permit content access.

Supported in the following platforms:

- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
http-access precedence <1-100> [deny|permit] {destination-domain
<DOMAIN-NAME>|
          destination-domain-regex <WORD>|destination-ip <IP>|mimetype-regex
<WORD>|
          source-ip <IP>|url-regex <URL>}
```

Parameters

```
http-access precedence <1-100> [deny|permit] {destination-domain
<DOMAIN-NAME>|
destination-domain-regex <WORD>|destination-ip <IP>|mimetype-regex <WORD>|
source-ip <IP>|url-regex <URL>}
```

http-access precedence <1-100>	Configures HTTP access rules that determine if a IP address is to be accessed or not. You can create multiple HTTP access rules and assign precedence values to each. These rules are applied in order of their precedence. • <1-100> – Specify a precedence rule from 1 - 100. Lower the precedence, higher is the rule priority.
[deny|permit]	Configures the deny or permit access parameters for this rule • permits – Permits access if the specified parameters are matched • deny – Denies access if the specified parameters are matched
destination-domain <DOMAIN-NAME>	Optional. Specifies the destination domain to match against the hostname in the HTTP request URL
destination-domain-regex <WORD>	Optional. Specifies a regular expression matching on originating server names The destination domain regex is the same as the destination domain, but the destination domain regex allows your to use standard expression matching on originating server names.
destination-ip [<IP>/M|any]	Optional. Specifies the originating server's IP address, obtained from the HTTP request URL Provide the IP address in the A.B.C.D/M format. Specify *any* to consider all originating servers.
mimetype-regex <WORD>	Optional. Specifies the regular expression used to match the mimetype of a HTTP request
source-ip [<IP>/M|any]	Optional. Specifies the source IP address (client's IP address) that is sent out as part of the HTTP request. Provide the IP address in the A.B.C.D/M format. Specify *any* to consider all client requests.
url-regex <URL>	Optional. Specifies regular expressions used to match any part of a requested URL, including the transfer protocol and originating server hostname

Example

```
nx4500-5CFA2B(config-smart-cache-policy-test)#http-access precedence 4 deny
destination-domain .TechPubs
nx4500-5CFA2B(config-smart-cache-policy-test)#

nx4500-5CFA2B(config-smart-cache-policy-test)#show context
smart-cache-policy test
 forward-proxy vlan 10-20
```

```
 cache size 30
 aging precedence 1 ignore-case \\.jgp$ min-age 100 freshness-factor 75
max-age 200 reload-into-ims
 http-access precedence 4 deny destination-domain .TechPubs
 access-log rotate 10 rotate-type duration 10 day
nx4500-5CFA2B(config-smart-cache-policy-test)#
```

Related Commands:

no	Removes an ACL

no

smart-cache-policy-mode commands

Removes or resets smart cache policy settings

Supported in the following platforms:

- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no [access-log|aging|cache|forward-proxy|http-access|parent-proxy|pre-fetch|
          smart-cache|transparent-proxy]
```

Parameters

```
no
[access-log|aging|cache|forward-proxy|http-access|parent-proxy|pre-fetch|smar
t-cache|transparent-proxy]
```

no access-log	Disables logging of all client requests
no aging	Removes the refresh pattern configured with this smart cache policy
no cache	Removes cache management settings
no forward-proxy	Removes the forward proxy settings
no http-access	Removes the ACL associated with this smart cache policy
no parent-proxy	Removes the parent proxy settings
no pre-fetch	Disables pre-fetching of a URL
no smart-cache	Disables smart content caching
no transparent-proxy	Removes the transparent proxy settings

Example

```
The following example displays the content cache policy ‘test’ settings before
the no commands are executed:

nx4500-5CFA2B(config-smart-cache-policy-test)#show context
smart-cache-policy test
 forward-proxy vlan 10-20
 cache size 30
 aging precedence 1 ignore-case \\.jgp$ min-age 100 freshness-factor 75
max-age 200 reload-into-ims
 http-access precedence 4 deny destination-domain .TechPubs
 access-log rotate 10 rotate-type duration 10 day
nx4500-5CFA2B(config-smart-cache-policy-test)#
```

```
nx4500-5CFA2B(config-content-cache-policy-test)#no forward-proxy vlan 10-20
nx4500-5CFA2B(config-smart-cache-policy-test)#no aging precedence 1
nx4500-5CFA2B(config-smart-cache-policy-test)#no access-log rotate

The following example displays the content cache policy ‘test’ settings after
the no commands are executed:

nx4500-5CFA2B(config-smart-cache-policy-test)#show context
smart-cache-policy test
 cache size 30
 http-access precedence 4 deny destination-domain .TechPubs
nx4500-5CFA2B(config-smart-cache-policy-test)#
```

pre-fetch

smart-cache-policy-mode commands

Pre-fetches a specified list of URLs (whose credentials can be stored in the local cache)

This command allows the content cache engine to pre-fetch URLs specified in a URL list. The pre-fetch function is performed immediately or at a scheduled time, based on configuration.

Supported in the following platforms:

- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
pre-fetch <URL-LIST-NAME> schedule <TIME>
```

Parameters

```
pre-fetch <URL-LIST-NAME> schedule <TIME>
```

<URL-LIST-NAME>	Pre-fetches a list of URLs identified by the <URL-LIST-NAME> keyword. URL lists are used to select highly utilized URLs for smart caching. The selected URLs are monitored and routed according to existing cache content policies. The URL list should be existing and configured. For more information on configuring URL lists, see .
schedule <TIME>	Pre-fetches the specified URL list at a specified time • <TIME> – Specify the time in the HH:MM format.

Example

```
nx4500-5CFA2B(config-content-cache-policy-test)#pre-fetch test schedule 12:30
nx4500-5CFA2B(config-content-cache-policy-test)#

nx4500-5CFA2B(config-content-cache-policy-test)#show context
content-cache-policy test
 forward-proxy vlan 10-20
 cache media all
 cache size 30
 http-access precedence 100 deny destination-domain test
destination-domain-regex test
 access-log rotate 10 every 50 day
 pre-fetch test schedule 12:30
nx4500-5CFA2B(config-content-cache-policy-test)#
```

Related Commands:

no	Removes an ACL

parent-proxy

smart-cache-policy-mode commands

Enables or disables upper-layer parent proxy on this smart cache policy

The parent proxy server requires users to authenticate to access Web sites like WinRoute. This setting is disabled by default.

Supported in the following platforms:

- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
parent-proxy [enable|host <IP/HOST-NAME> port <1-32768>]
```

Parameters

```
parent-proxy [enable|host <IP/HOST-NAME> port <1-32768>]
```

enable	Enables parent proxy on this smart cache policy
host <IP/HOST-NAME> port <1-32768>	Configures the hostname or IP address of the parent proxy server • <IP/HOST-NAME> – Specify the parent proxy server's IP address or hostname. • port <> – Specify the TCP port number for the parent proxy server. The default port is 8080.

Example

```
nx4500-5CFA2B(config-smart-cache-policy-test)#parent-proxy host 192.168.13.8
port 21
nx4500-5CFA2B(config-smart-cache-policy-test)#

nx4500-5CFA2B(config-smart-cache-policy-test)#show context
smart-cache-policy test
 parent-proxy host 192.168.13.8 port 21
 cache size 30
 http-access precedence 4 deny destination-domain .TechPubs
nx4500-5CFA2B(config-smart-cache-policy-test)#
```

Related Commands:

no	Disables parent proxy on this smart cache policy

smart-cache

smart-cache-policy-mode commands

Enables smart content caching

Supported in the following platforms:

- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
smart-cache enable
```

Parameters

```
smart-cache enable
```

smart-cache enable	Enables smart content caching. When enabled, devices using this smart-cache policy act as forward proxy.

Example

```
nx4500-5CFA2B(config-smart-cache-policy-test)#smart-cache enable
nx4500-5CFA2B(config-smart-cache-policy-test)#
```

Related Commands:

no	Disables smart content caching

transparent-proxy

smart-cache-policy-mode commands

Enables or disables the transparent proxy mode on a device. This is the default mode of proxying.

When enabled, all packets are automatically routed to the port on which the content cache engine listens (3128) by default. The advantage of the transparent proxy mode is that clients need not be configured with an explicit proxy,

Transparent content caching, on the other hand, acts as an intermediary for the originating servers and returns cached content to clients as if the data originated from the associated servers. Transparent caching proxies perform server load-balancing and compression to regulate load on the originating servers and reduce bandwidth usage.

Supported in the following platforms:

- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
transparent-proxy {protocol|vlan}

transparent-proxy {protocol {all|https}}
transparent-proxy {vlan <VLAN-ID>}
```

Parameters

```
transparent-proxy {protocol {all|https}}
```

protocol {all|https}	Optional. Selects the protocols used for transparent proxy mode • https – Optional. Enables HTTPS for transparent proxy • all – Optional. Enables all protocols for transparent proxy

```
transparent-proxy {vlan <VLAN-IP>}
```

vlan <VLAN-ID>	Optional. Configures the VLAN(s) for which transparent proxy mode (content caching) is enabled. By default content caching is disabled on all VLANs. • <VLAN-ID> – Specify the list of VLANs.

Example

```
nx4500-5CFA2B(config-smart-cache-policy-test)#transparent-proxy vlan 10-20
nx4500-5CFA2B(config-smart-cache-policy-test)#

nx4500-5CFA2B(config-smart-cache-policy-test)#show context
smart-cache-policy test
```

```
 parent-proxy host 192.168.13.8 port 21
 transparent-proxy vlan 10-20
 cache size 30
 http-access precedence 4 deny destination-domain .TechPubs
nx4500-5CFA2B(config-smart-cache-policy-test)#
```

Related Commands:

no	Resets or removes transparent caching proxy settings

Chapter

COMMON COMMANDS 5

This chapter describes the CLI commands used in the USER EXEC, PRIV EXEC, and GLOBAL CONFIG modes.

The PRIV EXEC command set contains commands available within the USER EXEC mode. Some commands can be entered in either mode. Commands entered in either the USER EXEC or PRIV EXEC mode are referred to as EXEC mode commands. If a user or privilege is not specified, the referenced command can be entered in either mode.

Common Commands

Table 3 summarizes commands common to the User Exec, Priv Exec, and Global Config modes.

TABLE 3 Commands Common to Controller CLI Modes

Command	Description	Reference
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
exit	Ends and exits the current mode and moves to the PRIV EXEC mode	page 387
help	Displays the interactive help system	page 387
no	Negates a command or reverts values to their default settings	page 391
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 394
show	Displays running system information	page 423
write	Writes the system's running configuration to memory or terminal	page 425

clrscr

Common Commands

Clears the screen and refreshes the prompt, irrespective of the mode

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
clrscr
```

Parameters

None

Example

```
The terminal window or screen before the clrscr command is executed:

rfs4000-229D58#device-upgrade ?
  DEVICE-NAME     Name/MAC address of device
  all             Upgrade all devices
```

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — , Brocade Mobility RFS9510

```
 Device
  br650           Upgrade Brocade Mobility 650 Access Point Device
  br6511          Upgrade Brocade Mobility 6511 Access Point Device
  br1220          Upgrade Brocade Mobility 1220 Access Point Device
  br71xx          Upgrade Brocade Mobility 71XX Access Point Device
  br81xx          Upgrade Brocade Mobility 1240 Access Point Device
  cancel-upgrade  Cancel upgrading the device
   load-image      Load the device images to controller for device-upgrades
   rf-domain       Upgrade all devices belonging to an RF Domain
   rfs4000         Upgrade Brocade Mobility RFS4000 Device

rfs4000-229D58#

The terminal window or screen after the clrscr command is executed:
rfs4000-229D58#
```

commit

Common Commands

Commits changes made in the active session. Use the commit command to save and invoke settings entered during the current transaction.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
commit {write}{memory}
```

Parameters

```
commit {write}{memory}
```

write	Optional. If a commit succeeds, the configuration is written to memory
memory	Optional. Writes to memory

Example

```
rfs7000-37FABE#commit write memory
[OK]
rfs7000-37FABE#
```

exit

Common Commands

The exit command works differently in the User Exec, Priv Exec, and Global Config modes. In the Global Config mode, it ends the current mode and moves to the previous mode, which is Priv Exec mode. The prompt changes from `(config)# to #`. When used in the Priv Exec and User Exec modes, the exit command ends the current session, and connection to the terminal device is terminated. If the current session has changes that have not been committed, the system will prompt you to either do a commit or a revert before terminating the session.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — , Brocade Mobility RFS9510

```
exit
```

Parameters

None

Example

```
rfs7000-37FABE(config)#exit
rfs7000-37FABE#
```

help

Common Commands

Describes the interactive help system

Use this command to access the advanced help feature. Use “**?**” anytime at the command prompt to access the help topic

Two kinds of help are provided:

- Full help is available when ready to enter a command argument

- Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (for example 'show ve?').

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
help {search|show}

help {show configuration-tree}

help {search <WORD>} {detailed|only-show|skip-no|skip-show}
```

NOTE
The *show configuration-tree* option is not available in the Global Config mode.

Parameters

```
help {show configuration-tree}
```

show configuration-tree	Optional. Displays the running system information • configuration-tree – Displays relationship amongst configuration objects

```
help {search <WORD>} {detailed|only-show|skip-no|skip-show}
```

search <WORD>	Optional. Searches for CLI commands related to a specified target term • <WORD> – Specify a target term (for example, a feature or a configuration parameter). After specifying the term, select one of the following options: detailed, only-show, skip-no, or skip-show. The system displays information based on the option selected.
detailed	Optional. Searches and displays help strings in addition to mode and commands
only-show	Optional. Displays only “show” commands. Does not display configuration commands
skip-no	Optional. Displays only configuration commands. Does not display “no” commands
skip-show	Optional. Displays only configuration commands. Does not display “show” commands

Example

```
rfs7000-37FABE>help search crypto detailed
Found 29 references for “crypto”
      Found 113 references for “crypto”

Mode    : User Exec
Command : show crypto key rsa (|public-key-detail) (|(on DEVICE-NAME))
           \ Show running system information
            \ Encryption related commands
             \ Key management operations
              \ Show RSA public Keys
               \ Show the public key in PEM format
                \ On AP/Controller
                 \ AP / Controller name
```

```
        : show crypto pki trustpoints (WORD|all|)(|(on DEVICE-NAME))
                  \ Show running system information
                  \ Encryption related commands
                  \ Public Key Infrastructure related commands
                  \ Display the configured trustpoints
                  \ Display a particular trustpoint's details
                  \ Display details for all trustpoints
                  \ On AP/Controller
                   \ AP / Controller name

        : show crypto isakmp sa (|(on DEVICE-NAME))
                   \ Show running system information
                   \ Encryption Module
                   \ Show ISAKMP related statistics
                   \ Show all ISAKMP Security Associations
                   \ On AP/Controller
                   \ AP / Controller name

        : show crypto ipsec sa (|(on DEVICE-NAME))
                   \ Show running system information
                   \ Encryption Module
                   \ Show IPSec related statistics
                   \ IPSec security association
                   \ On AP/Controller
                   \ AP / Controller name

        : crypto key generate rsa WORD <1024-2048> (|(on DEVICE-NAME))
                   \ Encryption related commands
                   \ Key management operations
                   \ Generate a keypair
                   \ Generate a RSA keypair
                   \ Keypair name
.....................................................................
.......
rfs7000-37FABE>

rfs7000-37FABE>help show configuration-tree

 ## ACCESS-POINT / SWITCH ## ---+
                               |
                               +--> [[ RF-DOMAIN ]]
                               |
                               +--> [[ PROFILE ]]
                               |
                             +--> Device specific parameters (license, serial
number, hostname)
                               |
                               +--> Configuration Overrides of rf-domain and
profile

 ## RF-DOMAIN ## ---+
                   |
                   +--> RF parameters, WIPS server parameters
                   |
                   +--> [[ SMART-RF-POLICY ]]
                   |
                   +--> [[ WIPS POLICY ]]

 ## PROFILE ## ---+
                  |
```

```
                    +--> Physical interface (interface GE,ME,UP etc)
                    |                          |
                    |                         +--> [[ RATE-LIMIT-TRUST-POLICY ]]
                    |
                    +--> Vlan interface (interface VLAN1/VLAN36 etc)
                    |
                    +--> Radio interface (interface RADIO1, RADIO2 etc)
                    |                           |
                   |                           +--> Radio specific Configuration
                    |                           |
                    |                           +--> [[ RADIO-QOS-POLICY ]]
                    |                           |
                    |                           +--> [[ ASSOC-ACL-POLICY ]]
                    |                           |
                    |                           +--> [[ WLAN ]]
                    |
                    +--> [[ MANAGEMENT-POLICY ]]
                    |
                    +--> [[ DHCP-SERVER-POLICY ]]
                    |
                    +--> [[ FIREWALL-POLICY ]]
                    |
                    +--> [[ NAT-POLICY ]]
.....................................................................
.......
rfs7000-37FABE>

rfs7000-37FABE>help search clrscr only-show
found no commands containing "clrscr"
rfs7000-37FABE>

rfs7000-37FABE>help search service skip-show
Found 32 references for "service"

Mode    : User Exec
Command : service show cli
        : service show rim config (|include-factory)
        : service show wireless credential-cache
        : service show wireless neighbors
        : service show general stats(|(on DEVICE-OR-DOMAIN-NAME))
        : service show process(|(on DEVICE-OR-DOMAIN-NAME))
        : service show mem(|(on DEVICE-OR-DOMAIN-NAME))
        : service show top(|(on DEVICE-OR-DOMAIN-NAME))
        : service show crash-info (|(on DEVICE-OR-DOMAIN-NAME))
        : service cli-tables-skin
(none|minimal|thin|thick|stars|hashes|percent|ansi|utf-8) (grid|)
        : service cli-tables-expand (|left|right)
       : service wireless clear unauthorized aps (|(on DEVICE-OR-DOMAIN-NAME))
        : service wireless qos delete-tspec AA-BB-CC-DD-EE-FF tid <0-7>
        : service wireless wips clear-event-history
        : service wireless wips clear-mu-blacklist (all|(mac
AA-BB-CC-DD-EE-FF))
        : service radio <1-3> dfs simulate-radar (primary|extension)
        : service smart-rf run-calibration
        : service smart-rf stop-calibration
        : service cluster manual-revert
        : service advanced-wips clear-event-history
```

```
        : service advanced-wips clear-event-history
(dos-eap-failure-spoof|id-theft-out-of-sequence|id-theft-eapol-success-spoof-
detected|wlan-jack-attack-detected|essid-jack-attack-detected|monkey-jack-att
ack-detected|null-probe-response-detected|fata-jack-detected|fake-dhcp-server
-detected|crackable-wep-iv-used|windows-zero-config-memory-leak|multicast-all
-systems-on-subnet|multicast-all-routers-on-subnet|multicast-ospf-all-routers
-detection|multicast-ospf-designated-routers-detection|multicast-rip2-routers
-detection|multicast-igmp-routers-detection|multicast-vrrp-agent|multicast-hs
rp-agent|multicast-dhcp-server-relay-agent|multicast-igmp-detection|netbios-d
etection|stp-detection|ipx-detection|invalid-management-frame|invalid-channel
-advertized|dos-deauthentication-detection|dos-disassociation-detection|dos-r
ts-flood|rogue-br-detection|accidental-association|probe-response-flood|dos-c
ts-flood|dos-eapol-logoff-storm|unauthorized-bridge)
        : service start-shell
        : service pktcap on(bridge|drop|deny|router|wireless|vpn|radio
(all|<1-3>) (|promiscuous)|rim|interface `WORD|ge <1-4>|me1|pc <1-4>|vlan
<1-4094>')(|{direction (any|inbound|outbound)|acl-name WORD|verbose|hex|count
<1-1000000>|snap <1-2048>|write (FILE|URL|tzsp WORD)|tcpdump})(|filter LINE)

Mode    : Profile Mode
Command : service watchdog

Mode    : Radio Mode
Command : service antenna-type
(default|dual-band|omni|yagi|embedded|panel|patch|sector|out-omni|in-patch|AP
650-int)
        : service disable-erp
        : service disable-ht-protection
        : service recalibration-interval <0-65535>
.....................................................................
rfs7000-37FABE>

rfs7000-37FABE>help search mint only-show
Found 8 references for "mint"

Mode    : User Exec
Command : show mint neighbors (|details)(|(on DEVICE-NAME))
        : show mint links (|details)(|(on DEVICE-NAME))
        : show mint id(|(on DEVICE-NAME))
        : show mint stats(|(on DEVICE-NAME))
        : show mint route(|(on DEVICE-NAME))
        : show mint lsp
        : show mint lsp-db (|details)(|(on DEVICE-NAME))
        : show mint mlcp(|(on DEVICE-NAME))
rfs7000-37FABE>
```

no

Common Commands

Negates a command or sets its default. Though the no command is common to the User Exec, Priv Exec, and Global Config modes, it negates a different set of commands in each mode.

Supported in the following platforms:s

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no <PARAMETER>
```

Parameters

None

Usage Guidelines:

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
Global Config mode: No command options
Enter configuration commands, one per line.  End with CNTL/Z.
rfs7000-37FABE(config)#no ?
  aaa-policy                  Delete a aaa policy
  aaa-tacacs-policy           Delete a aaa tacacs policy
  advanced-wips-policy        Delete an advanced-wips policy
  alias                       Alias
```

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — , Brocade Mobility RFS9510

```
 access point
br650                      Delete an Brocade Mobility 650 Access Point access
point
  br6511                      Delete an Brocade Mobility 6511 Access Point
access point
br1220                    Delete an Brocade Mobility 1220 Access Point access
point
br71xx                    Delete an Brocade Mobility 71XX Access Point access
point
  br81xx                      Delete an Brocade Mobility 1240 Access Point
access point
association-acl-policy      Delete an association-acl policy
  auto-provisioning-policy    Delete an auto-provisioning policy
  captive-portal              Delete a captive portal
  client-identity             Client identity (DHCP Device Fingerprinting)
  client-identity-group       Client identity group (DHCP Fingerprint
                              Database)
  customize                   Restore the custom cli commands to default
  device                      Delete multiple devices
  device-categorization       Delete  device categorization object
  dhcp-server-policy          DHCP server policy
  dns-whitelist               Delete a whitelist object
  event-system-policy         Delete a event system policy
```

```
  firewall-policy             Configure firewall policy
  global-association-list     Delete a global association list
  igmp-snoop-policy           Remove device onboard igmp snoop policy
  inline-password-encryption  Disable storing encryption key in the startup
                              configuration file
  ip                          Internet Protocol (IP)
  l2tpv3                      Negate a command or set its defaults
  mac                         MAC configuration
  management-policy           Delete a management policy
  meshpoint                   Delete a meshpoint object
  meshpoint-qos-policy        Delete a mesh point QoS configuration policy
  nac-list                    Delete an network access control list
  passpoint-policy            Delete a passpoint configuration policy

  password-encryption         Disable password encryption in configuration
  profile                     Delete a profile and all its associated
                              configuration
  radio-qos-policy            Delete a radio QoS configuration policy
  radius-group                Local radius server group configuration
  radius-server-policy        Remove device onboard radius policy
  radius-user-pool-policy     Configure Radius User Pool
  rf-domain                   Delete one or more RF-domains and all their
                              associated configurations
  rfs4000                     Delete an Brocade Mobility RFS4000 wireless
controller
  rfs6000                     Delete an Brocade Mobility RFS6000 wireless
controller
  rfs7000                     Delete an Brocade Mobility RFS7000 wireless
controller
  role-policy                 Role based firewall policy
  routing-policy              Policy Based Routing Configuration
  smart-rf-policy             Delete a smart-rf-policy
  wips-policy                 Delete a wips policy
  wlan                        Delete a wlan object
  wlan-qos-policy             Delete a wireless lan QoS configuration policy

  service                     Service Commands

rfs7000-37FABE(config)#

Priv Exec mode: No command options
rfs7000-37FABE#no ?
  adoption        Reset adoption state of the device (& all devices adopted to
                  it)
  captive-portal  Captive portal commands
  crypto          Encryption related commands
  debug           Debugging functions
  logging         Modify message logging facilities
  page            Toggle paging
  service         Service Commands
  terminal        Set terminal line parameters
  upgrade         Remove a patch
  wireless        Wireless Configuration/Statistics commands

rfs7000-37FABE#

user Exec mode: No command options
rfs7000-37FABE>no ?
  adoption        Reset adoption state of the device (& all devices adopted to
                  it)
```

```
  captive-portal  Captive portal commands
  crypto          Encryption related commands
  debug           Debugging functions
  logging         Modify message logging facilities
  page            Toggle paging
  service         Service Commands
  terminal        Set terminal line parameters
  wireless        Wireless Configuration/Statistics commands

rfs7000-37FABE>
```

Related Commands:

no	User Exec Commands mode
no	Priv Exec Commands mode
no	Global Config Commands mode

revert

Common Commands

Reverts changes made, in the current session, to their last saved configuration

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
revert
```

Parameters

None

Example

```
rfs7000-37FABE>revert
rfs7000-37FABE>
```

service

Common Commands

Service commands are used to view and manage configurations. The service commands and their corresponding parameters vary from mode to mode. The User Exec mode and Priv Exec mode commands provide same functionalities with a few minor changes. The Global Config service command sets the size of history files. It also enables viewing the current mode's CLI tree.

This section consists of the following sub-sections:

- Syntax *(User Exec Mode)*
- Syntax *(Privilege Exec Mode)*
- Syntax (Privilege Exec Mode: Brocade Mobility RFS9510)
- Syntax *(Global Config Mode)*

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax: (User Exec Mode)

```
service [advanced-wips|block-adopter-config-update|clear|cli-tables-skin|

cluster|delete-offline-aps|force-send-config|force-update-vm-stats|load-balan
cing|

locator|radio|radius|request-full-config-from-adopter|set|show|smart-rf|ssm|
          wireless]

service advanced-wips [clear-event-history|terminate-device <MAC>]

service advanced-wips clear-event-history {accidental-association|
          crackable-wep-iv-used|dos-cts-flood|dos-deauthentication-detection|

dos-disassociation-detection|dos-eap-failure-spoof|dos-eapol-logoff-storm|
          dos-rts-flood|essid-jack-attack-detected|fake-dhcp-server-detected|

fata-jack-detected|id-theft-eapol-success-spoof-detected|id-theft-out-of-sequ
ence|
          invalid-channel-advertized|invalid-management-frame|ipx-detection|
          monkey-jack-attack-detected|multicast-all-routers-on-subnet|
          multicast-all-systems-on-subnet|multicast-dhcp-server-relay-agent|

multicast-hsrp-agent|multicast-igmp-detection|multicast-igrp-routers-detectio
n|

multicast-ospf-all-routers-detection|multicast-ospf-designated-routers-detect
ion|

multicast-rip2-routers-detection|multicast-vrrp-agent|netbios-detection|

null-probe-response-detected|probe-response-flood|rogue-br-detection|
          stp-detection|unauthorized-bridge|windows-zero-config-memory-leak|
          wlan-jack-attack-detected}

service [block-adopter-config-update|request-full-config-from-adopter]

service clear [adoption|captive-portal-page-upload|command-history|
          device-upgrade|noc|reboot-history|unsanctioned|upgrade-history|
          virtual-machine-history|wireless|xpath]

service clear adoption history {on <DEVICE-NAME>}
```

```
service clear device-upgrade history {on <DOMAIN-NAME>}
service clear captive-portal-page-upload history {on <DOMAIN-NAME>}
service clear
[command-history|reboot-history|upgrade-history|virtual-machine-history]
          {on <DEVICE-NAME>}
service clear noc statistics
service clear unsanctioned aps {on <DEVICE-OR-DOMAIN-NAME>}

service clear wireless
[br|client|controller-mobility-database|dns-cache|radio|wlan]
service clear wireless controller-mobility-database
service clear wireless [br|client] statistics {<MAC>} {(on
<DEVICE-OR-DOMAIN-NAME>)}
service clear wireless dns-cache on {(on <DEVICE-OR-DOMAIN-NAME)}
service clear wireless radio statistics {<MAC/HOSTNAME>} {<1-3>} {(on
<DEVICE-OR-DOMAIN-
          NAME>)}
service clear wireless wlan statistics {<WLAN-NAME>} {(on
<DEVICE-OR-DOMAIN-NAME)}
service clear xpath requests {<1-100000>}

service cli-tables-skin
[ansi|hashes|minimal|none|percent|stars|thick|thin|utf-8]
          {grid}

service cluster force [active|configured-state|standby]

service delete-offline-aps [all|offline-for]
service delete-offline-aps offline-for days <0-999> {time <TIME>}

service enable [l2tpv3|radiusd]

service force-send-config {on <DEVICE-OR-DOMAIN-NAME>}

service force-update-vm-stats {on <DEVICE-NAME>}

service load-balancing clear-client-capability [<MAC>|all] {on <DEVICE-NAME>}

service locator {<1-60>} {(on <DEVICE-NAME>)}

service radio <1-3> dfs simulator-radar [extension|primary]

service radius test [<IP>|<HOSTNAME>] [<WORD>|<PORT>]
service radius test [<IP>|<HOSTNAME>] <WORD> <USERNAME> <PASSWORD> {wlan
<WLAN-NAME>
          ssid <SSID>} {(on <DEVICE-NAME>)}
service radius test [<IP>|<HOSTNAME>] <PORT> <1024-65535> <WORD> <USERNAME>
          <PASSWORD> {wlan <WLAN-NAME> ssid <SSID>} {(on <DEVICE-NAME>)}

service set validation-mode [full|partial] {on <DEVICE-NAME>}

service show [advanced-wips|block-adopter-config-update|captive-portal|cli|

command-history|configuration-revision|crash-info|dhcp-lease|diag|fast-switch
ing|

fib|hardware-switch|info|mac-vendor|mem|mint|noc|pm|process|reboot-history|

rf-domain-manager|sites|snmp|startup-log|sysinfo|top|upgrade-history|
          virtual-machine-history|watch-dog|wireless|xpath-history]
```

```
service show advanced-wips stats
[br-table|client-table|connected-sensors-status|
          termination-entries]
service show block-adopter-config-update
service show captive-portal [servers|user-cache] {on <DEVICE-NAME>}
service show [cli|configuration-revision|mac-vendor <OUI/MAC>|noc diag|snmp
session|
          xpath-history]
service show [command-history|crash-info|info|mem|process|reboot-history|
          startup-log|sysinfo|top|upgrade-history|watchdog] {on
<DEVICE-NAME>}
service show dhcp-lease {<INTERFACE-NAME>|pppoe1|vlan <1-4094>|wwan1}
          {(on <DEVICE-NAME>)}
service show diag [led-status|stats] {on <DEVICE-NAME>}
service show fast-switching {on <DEVICE-NAME>}
service show fib {table-id <0-255>}
service show hardware-switch mac-address-table
service show mint [adopted-devices {on <DEVICE-NAME>}|ports]
service show pm {history} {(on <DEVICE-NAME>)}
service show rf-domain-manager diag {<MAC/HOSTNAME>} {(on
<DEVICE-OR-DOMAIN-NAME>)}
service show sites

service show virtual-machine-history {on <DEVICE-NAME>}

service show wireless [aaa-stats|client|config-internal|credential-cache|

dns-cache|log-internal|meshpoint|neighbors|reference|stats-client|vlan-usage]
service show wireless [aaa-stats|credential-cache|dns-cache|vlan-usage]
          {on <DEVICE-NAME>}
service show wireless [config-internal|log-internal|neighbors]
service show wireless [client|meshpoint neighbor] proc [info|stats] {<MAC>}
          {{on <DEVICE-OR-DOMAIN-NAME>)}
service show wireless reference dot11 [frame|handshake|mcs-rates|reason-codes|
          status-codes]
service show wireless reference dot11 handshake {wpa-wpa2-enterprise|
          wpa-wpa2-personal}
service show wireless stats-client diag {<MAC/HOSTNAME>} {(on
<DEVICE-OR-DOMAIN-
          NAME>)}

service smart-rf [clear-config|clear-history|interactive-calibration|

interactive-calibration-result|run-calibration|save-config|stop-calibration]
service smart-rf clear-config {<MAC>|<DEVICE-NAME>|on <DOMAIN-NAME>}
service smart-rf
[clear-history|interactive-calibration|run-calibration|save-config|
          stop-calibration] {on <DOMAIN-NAME>}
service smart-rf interactive-calibration-result
[discard|replace-current-config|
          write-to-configuration] {on <DOMAIN-NAME>}

service ssm [dump-core-snapshot|trace]
service ssm trace pattern <WORD> {on <DEVICE-NAME>}

service wireless [client|dump-core-snapshot|meshpoint|qos|trace|wips]

service wireless client [beacon-request|quiet-element|trigger-bss-transition]
```

```
service wireless client beacon-request <MAC> mode [active|passive|table]
          ssid [<SSID>|any] channel-report [<CHANNEL-LIST>|none] {on
<DEVICE-NAME>}
service wireless client quiet-element [start|stop]
service wireless client trigger-bss-transition <MAC> url <URL> {on
<DEVICE-OR-DOMAIN-
          NAME>}
service wireless dump-core-snapshot
service wireless meshpoint zl <MESHPOINT-NAME> [on <DEVICE-NAME>] {<ARGS>}
service wireless qos delete-tspec <MAC> tid <0-7>
service wireless trace pattern <WORD> {on <DEVICE-NAME>}
service wireless wips [clear-client-blacklist|clear-event-history|
          dump-managed-config]
service wireless wips clear-client-blacklist [all|mac <MAC>]
service wireless wips clear-event-history {on <DEVICE-OR-DOMAIN-NAME>}
```

Parameters (User Exec Mode)

service

```
service advanced-wips clear-event-history {accidental-association|
crackable-wep-iv-used|dos-cts-flood|dos-deauthentication-detection|
dos-disassociation-detection|dos-eap-failure-spoof|dos-eapol-logoff-storm|
dos-rts-flood|essid-jack-attack-detected|fake-dhcp-server-detected|
fata-jack-detected|id-theft-eapol-success-spoof-detected|
id-theft-out-of-sequence|invalid-channel-advertized|invalid-management-frame|
ipx-detection|monkey-jack-attack-detected|multicast-all-routers-on-subnet|
multicast-all-systems-on-subnet|multicast-dhcp-server-relay-agent|
multicast-hsrp-agent|multicast-igmp-detection|multicast-igrp-routers-detectio
n|
multicast-ospf-all-routers-detection|multicast-ospf-designated-routers-detect
ion|
multicast-rip2-routers-detection|multicast-vrrp-agent|netbios-detection|
null-probe-response-detected|probe-response-flood|rogue-br-detection|stp-dete
ction|
unathorized-bridge|windows-zero-config-memory-leak|wlan-jack-attack-detected}
```

advanced-wips clear-event-history	The advanced *Wireless Intrusion Prevention System* (WIPS) service command clears event history and terminates a device. • clear-event-history – Clears event history based on the parameters passed
accidental-association	Optional. Clears accidental wireless client association event history
crackable-wep-iv-used	Optional. Clears crackable *Wired Equivalent Privacy* (WEP) IV used event history
dos-cts-flood	Optional. Clears DoS *Clear-To-Send* (CTS) flood event history
dos-deauthentication-detection	Optional. Clears DoS de-authentication detection event history
dos-disassociation-detection	Optional. Clears DoS disassociation detection event history
dos-eap-failure-spoof	Optional. Clears DoS *Extensible Authentication Protocol* (EAP) failure spoof detection event history
dos-eapol-logoff-storm	Optional. Clears DoS *Extensible Authentication Protocol over LAN* (EAPoL) logoff storm detection event history
dos-rts-flood	Optional. Clears DoS *request-to-send* (RTS) flood detection event history
essid-jack-attack-detected	Optional. Clears *Extended Service Set ID* (ESSID) jack attacks detection event history
fake-dhcp-server-detected	Optional. Clears fake DHCP server detection event history
fata-jack-detected	Optional. Clears fata-jack attacks detection event history

id-theft-eapol-success-spoof-detected	Optional. Clears IDs theft - EAPOL success spoof detection event history
id-theft-out-of-sequence	Optional. Clears IDs theft-out-of-sequence detection event history
invalid-channel-advertized	Optional. Clears invalid channel advertizement detection event history
invalid-management-frame	Optional. Clears invalid management frames detection event history
ipx-detection	Optional. Clears automatic IPX interface detection event history
monkey-jack-attack-detected	Optional. Detects monkey-jack attacks detection event history
multicast-all-routers-on-subnet	Optional. Clears all multicast routers on the subnet detection event history
multicast-all-systems-on-subnet	Optional. Clears all multicast systems on the subnet detection event history
multicast-dhcp-server-relay-agent	Optional. Clears multicast DHCP server relay agents detection event history
multicast-hsrp-agent	Optional. Clears multicast *Hot Standby Router Policy* (HSRP) agents detection event history
multicast-igmp-detection	Optional. Clears multicast *Internet Group Management Protocol* (IGMP) detection event history
multicast-igrp-routers-detection	Optional. Clears multicast *Interior Gateway Router Protocol* (IGRP) routers detection event history
multicast-ospf-all-routers-detection	Optional. Clears multicast *Open Shortest Path First* (OSPF) all routers detection event history
multicast-ospf-designated-routers-detection	Optional. Clears multicast OSPF designated routers detection event history
multicast-rip2-routers-detection	Optional. Clears multicast *Routing Information Protocol Version 2* (RIP2) routers detection event history
multicast-vrrp-agent	Optional. Clears multicast *Virtual Router Redundancy Protocol* (VRRP) agents detection event history
netbios-detection	Optional. Clears NetBIOS detection event history
null-probe-response-detected	Optional. Clears null probe response detection event history
probe-response-flood	Optional. Clears probe response flood detection event history
rogue-br-detection	Optional. Clears rogue AP detection event history
stp-detection	Optional. Clears *Spanning Tree Protocol* (STP) detection event history
unauthorized-bridge	Optional. Clears unauthorized bridge detection event history
windows-zero-config-memory-leak	Optional. Clears Windows zero configuration memory leak detection event history
wlan-jack-attack-detected	Optional. Clears WLAN jack attack detection event history

`service advanced-wips terminate-device <MAC>`

advanced-wips terminate-device <MAC>	The advanced WIPS service command clears event history details, and terminates a device. • terminate-device – Terminates a specified device • <MAC> – Specify the MAC address of the AP, wireless client, or service platform.

	`service [block-adopter-config-update|request-full-config-from-adopter]`
block-adopter-config-update	Blocks the configuration updates sent from the NOC server
request-full-config-from-adpoter	Configures a request for full configuration updates from the adopter device In an *hierarchically managed* (HM) network devices are deployed in two levels. The first level consists of the *Network Operations Center* (NOC) controllers. The second level consists of the site controllers that can be grouped to form clusters. The NOC controllers adopt and manage the site controllers. Access points within the network are adopted and managed by the site controllers. The adopted devices (access points and site controllers) are referred to as the adoptee. The devices adopting the adoptee are the 'adopters'.

	`service clear adoption history` *{on <DEVICE-NAME>}*
clear adoption history	Clears adoption history on this device and its adopted access points
on <DEVICE-NAME>	Optional. Clears adoption history on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

	`service clear device-upgrade history` *{on <DOMAIN-NAME>}*
clear device-upgrade history	Clears device upgrade history
on <DOMAIN-NAME>	Optional. Clears all firmware upgrade history in a specified RF Domain • <DOMAIN-NAME> – Specify the RF Domain name.

	`service clear captive-portal-page-upload history` *{on <DOMAIN-NAME>}*
clear captive-portal-page-upload history	Clears captive portal page upload history
on <DOMAIN-NAME>	Optional. Clears captive portal page upload history on a specified RF Domain • <DOMAIN-NAME> – Specify the RF Domain name.

	`service clear [command-history|reboot-history|upgrade-history|virtual-machine-history]` *{on <DEVICE-NAME>}*
clear [command-history|reboot-history|upgrade-history]	Clears command history, reboot history, or device upgrade history
clear virtual-machine-history	Clears virtual-machine history on the logged device or a specified device This command is applicable only on the Brocade Mobility RFS9510 series service platforms.
on <DEVICE-NAME>	Optional. Clears history on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. When executing the clear virtual-machine-history command, provide the name of the service platform running the VMs.

	`service clear noc statistics`
clear noc statistics	Clears *Network Operations Center* (NOC) applicable statistics counters

	`service clear unsanctioned aps` *{on <DEVICE-OR-DOMAIN-NAME>}*
clear unsanctioned aps	Clears the unsanctioned APs list
on <DEVICE-OR-DOMAIN-NAME>	Optional. Clears the unsanctioned APs list on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

	`service clear wireless [br|client] {<MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}`
clear wireless [br|client] statistics	Clears wireless statistics counters based on the parameters passed • br statistics – Clears applicable AP statistics counters • client statistics – Clears applicable wireless client statistics counters
<MAC> {on <DEVICE-OR-DOMAIN-NAME>}	The following keywords are common to the 'br' and 'client' parameters: • <MAC> – Optional. Clears statistics counters for a specified AP or client. Specify the AP/client MAC address. • on <DEVICE-OR-DOMAIN-NAME> – Optional. Clears AP/client statistics counters on a specified device or RF Domain. Specify the name of the AP, wireless controller, service platform, or RF Domain.

	`service clear wireless controller-mobility-database`
clear wireless controler-mobility-database	Clears the controller assisted mobility database

	`service clear wireless radio statistics {<MAC/HOSTNAME>} {<1-3>} {(on <DEVICE-OR-DOMAIN-NAME>)}`
clear wireless radio statistics	Clears applicable wireless radio statistics counters
<MAC/HOSTNAME> <1-3>	Optional. Specify the MAC address or hostname of the radio, or append the interface number to form the radio ID in the AA-BB-CC-DD-EE-FF:RX or HOSTNAME:RX format. • <1-3> – Optional. Specify the radio interface index, if not specified as part of the radio ID.
on <DEVICE-OR-DOMAIN-NAME>	Optional. This is a recursive parameter, which clears wireless radio statistics on a specified device or RF Domain. Specify the name of the AP, wireless controller, service platform, or RF Domain.

	`service clear wireless wlan statistics {<WLAN-NAME>} {(on <DEVICE-OR-DOMAIN-NAME>)}`
clear wireless wlan statistics	Clears WLAN statistics counters
<WLAN-NAME>	Optional. Clears statistics counters on a specified WLAN. Specify the WLAN name.
on <DEVICE-OR-DOMAIN-NAME>	Optional. This is a recursive parameter, which clears WLAN statistics on a specified device or RF Domain. Specify the name of the AP, wireless controller, service platform, or RF Domain.

	`service clear xpath requests {<1-100000>}`
clear xpath	Clears XPATH related information
requests	Clears pending XPATH get requests
<1-100000>	Optional. Specifies the session number (cookie from show sessions) • <1-100000> – Specify the session number from 1 - 100000. **NOTE:** Omits for this session

`service cli-tables-skin [ansi|hashes|minimal|none|percent|stars|thick|thin|utf-8] {grid}`

cli-tables-skin [ansi|hashes|minimal|none|percent|stars|thick|thin|uf-8]	Selects a formatting layout or skin for CLI tabular outputs • ansi – Uses ANSI characters for borders • hashes – Uses hashes (#) for borders • minimal – Uses one horizontal line between title and data rows • none – Displays space separated items with no decoration • percent – Uses the percent sign (%) for borders • stars – Uses asterisks (*) for borders • thick – Uses thick lines for borders • thin – Uses thin lines for borders • utf-8 – Uses UTF-8 characters for borders
grid	Optional. Uses a complete grid instead of just title lines

`service cluster force [active|configured-state|standby]`

cluster	Enables cluster protocol management
force	Forces action commands on a cluster (active, configured-state, and standby)
active	Changes the cluster run status to active
configured-state	Restores a cluster to the configured state
standby	Changes the cluster run status to standby

`service delete-offline-aps all`

delete-offline-aps all	Deletes all off-line access points

`service delete-offline-aps offline-for days <0-999> {time <TIME>}`

delete-offline-aps	Deletes off-line access points for a specified interval
day <0-999>	Deletes off-line access points for a specified number of days • <0-999> – Specify the number of off-line days from 0 - 999.
time <TIME>	Optional. Deletes off-line access points for a specified time • <TIME> – Specify the time in HH:MM:SS format.

`service enable [l2tpv3|radiusd]`

enable l2tpv3	Enables L2TPv3 on low memory devices
enable radiusd	Enables RADIUS server loading on low memory devices

`service force-send-config {on <DEVICE-OR-DOMAIN-NAME>}`

force-send-config	Resends configuration to device(s)
on <DEVICE-OR-DOMAIN-NAME>	Optional. Resends configuration to a specified device or all devices in a specified RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

`service force-update-vm-stats {on <DEVICE-NAME>}`

force-update-vm-stats	Forcefully pushes VM statistics on to the NOC
on <DEVICE-NAME>	Optional. Executes the command on a specified device • <DEVICE-NAME> – Specify the name of the device.

	`service load-balancing clear-client-capability [<MAC>|all] {on <DEVICE-NAME>}`
load-balancing	Enables wireless load balancing by clearing client capability records
clear-client-capability [<MAC>|all]	Clears a specified client or all client's capability records • <MAC> – Clears capability records of a specified client. Specify the client's MAC address in the AA-BB-CC-DD-EE-FF format. • all – Clears the capability records of all clients
on <DEVICE-NAME>	Optional. Clears client capability records on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

	`service locator {<1-60>} {(on <DEVICE-NAME>)}`
locator	Enables LEDs
<1-60>	Sets LED flashing time from 1 - 60 seconds.
on <DEVICE-NAME>	The following keyword is recursive and common to the <1-60> parameter: • on <DEVICE-NAME> – Optional. Enables LEDs on a specified device • <DEVICE-NAME> – Specify name of the AP, wireless controller, or service platform.

	`service radio <1-3> dfs simulate-radar [extension|primary]`
radio <1-3>	Configures radio's parameters • <1-3> – Specify the radio index from 1 - 3.
dfs	Enables *Dynamic Frequency Selection* (DFS)
simulate-radar [extension|primary]	Simulates the presence of a radar on a channel. Select the channel type from the following options: • extension – Simulates a radar on the radio's current extension channel • primary – Simulates a radar on the radio's current primary channel

	`service radius test [<IP>|<HOSTNAME>] <WORD> <USERNAME> <PASSWORD> {wlan <WLAN-NAME> ssid <SSID>} {(on <DEVICE-NAME>)}`
radius test	Tests RADIUS server's account. This command sends an access-request packet to the RADIUS server. Use this command to confirm time and data/bandwidth parameters for valid wireless clients. • test – Tests the RADIUS server's account with user provided parameters
[<IP>|<HOSTNAME>]	Sets the RADIUS server's IP address or hostname • <IP> – Specifies the RADIUS server's IP address • <HOSTNAME> – Specifies the RADIUS server's hostname
<WORD>	Specify the RADIUS server's shared secret.
<USERNAME>	Specify username for authentication.
<PASSWORD>	Specify the password.
wlan <WLAN-NAME> ssid <SSID>	Optional. Tests the RADIUS server on the local WLAN. Specify the local WLAN name. • ssid <SSID> – Specify the local RADIUS server's SSID.
on <DEVICE-NAME>	Optional. This is a recursive parameter also applicable to the WLAN parameter. Performs tests on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

	`service radius test [<IP>|<HOSTNAME>] <PORT> <1024-65535> <WORD> <USERNAME> <PASSWORD> {wlan <WLAN-NAME> ssid <SSID>} {(on <DEVICE-NAME>)}`
radius test	Tests a RADIUS server's account. This command sends an access-request packet to the RADIUS server. Use this command to confirm time and data/bandwidth parameters for valid wireless clients. • test – Tests the RADIUS server's account with user provided parameters
[<IP>|<HOSTNAME>]	Sets the IP address or hostname of the RADIUS server • <IP> – Specify the RADIUS server's IP address. • <HOSTNAME> – Specify the RADIUS server's hostname.
<PORT> <1024-65535>	Specify the RADIUS server port from 1024 - 65535. The default port is 1812.
<WORD>	Specify the RADIUS server's shared secret.
<USERNAME>	Specify username for authentication.
<PASSWORD>	Specify the password.
wlan <WLAN-NAME> ssid <SSID>	Optional. Tests the RADIUS server on the local WLAN. Specify the local WLAN name. • ssid <SSID> – Specify the RADIUS server's SSID.
on <DEVICE-NAME>	Optional. This is a recursive parameter also applicable to the WLAN parameter. Performs tests on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

	`service set validation-mode [full|partial] {on <DEVICE-NAME>}`
set	Sets the validation mode for running configuration validation
validation-mode [full|partial]	Sets the validation mode • full – Performs a full configuration validation • partial – Performs a partial configuration validation
on <DEVICE-NAME>	Optional. Performs full or partial configuration validation on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

	`service show advanced-wips stats [br-table|client-table|connected-sensors-status| termination-entries]`
show	Displays running system statistics based on the parameters passed
advanced-wips stats	Displays advanced WIPS statistics
br-table	Displays AP table statistics
client-table	Displays client table statistics
connected-sensors-status	Displays connected sensor statistics
termination-entries	Displays termination entries statistics

	`service show block-adopter-config-update]`
show	Displays running system statistics based on the parameters passed
block-adopter-config-update	Displays NOC configuration blocking status

	`service show captive-portal [servers|user-cache] {on <DEVICE-NAME>}`
show	Displays running system statistics based on the parameters passed
captive-portal	Displays captive portal information
servers	Displays server information for active captive portals

user-cache	Displays cached user details for a captive portal
on <DEVICE-NAME>	Optional. Displays server information or cached user details on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`service show [cli|configuration-revision|mac-vendor <OUI/MAC>|noc diag|snmp session|`
`xpath-history]`

show	Displays running system statistics based on the parameters passed
cli	Displays CLI tree of the current mode
configuration-revision	Displays current configuration revision number
mac-vendor <OUI/MAC>	Displays vendor name for a specified MAC address or *Organizationally Unique Identifier* (OUI) part of the MAC address • <OUI/MAC> – Specify the MAC address or its OUI. The first six digits of the MAC address is the OUI. Use the AABBCC or AA-BB-CC format to provide the OUI.
noc diag	Displays NOC diagnostic details
snmp session	Displays SNMP session details
xpath-history	Displays XPath history

`service show [command-history|crash-info|info|mem|process|reboot-history|`
`startup-log|sysinfo|top|upgrade-history|watchdog] {on <DEVICE-NAME>}`

show	Displays running system statistics based on the parameters passed
command-history	Displays command history (lists all commands executed)
crash-info	Displays information about core, panic, and AP dump files
info	Displays snapshot of available support information
mem	Displays a system's current memory usage (displays the total memory and available memory)
process	Displays active system process information (displays all processes currently running on the system)
reboot-history	Displays the device's reboot history
startup-log	Displays the device's startup log
sysinfo	Displays system's memory usage information
top	Displays system resource information
upgrade-history	Displays the device's upgrade history (displays details, such as date, time, and status of the upgrade, old version, new version etc.)
watchdog	Displays the device's watchdog status
on <DEVICE-NAME>	The following keywords are common to all of the above: • on <DEVICE-NAME> – Optional. Displays information for a specified device. If no device is specified, the system displays information for logged device(s) • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`service show dhcp-lease {<INTERFACE-NAME>|on|pppoe1|vlan <1-4094>|wwan1}`
`{(on <DEVICE-NAME>)}`

show	Displays running system statistics based on the parameters passed
dhcp-lease	Displays DHCP lease information received from the server
<INTERFACE>	Optional. Displays DHCP lease information for a specified router interface • <INTERFACE> – Specify the router interface name.

on	Optional. Displays DHCP lease information for a specified device
pppoe1	Optional. Displays DHCP lease information for a PPP over Ethernet interface
vlan <1-4094>	Optional. Displays DHCP lease information for a VLAN interface • <1-4094> – Specify a VLAN index from 1 - 4094.
wwan1	Optional. Displays DHCP lease information for a Wireless WAN interface
on <DEVICE-NAME>	The following keywords are common to all of the above: • on <DEVICE-NAME> – Optional. Displays DHCP lease information for a specified device. If no device is specified, the system displays information for the logged device. • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`service show diag [led-staus|stats] {(on <DEVICE-NAME>)}`

show	Displays running system statistics based on the parameters passed
diag	Displays diagnostic statistics, such as LED status, fan speed, and sensor temperature
led-status	Displays LED state variables and the current state
stats	Displays fan speed and sensor temperature statistics
on <DEVICE-NAME>	Optional. Displays diagnostic statistics for a specified device. If no device is specified, the system displays information for the logged device. • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`service show fib {table-id <0-255>}`

show	Displays running system statistics based on the parameters passed
fib	Displays entries in the *Forwarding Information Base* (FIB)
table-id <0-255>	Optional. Displays FIB information maintained by the system based on the table ID • <0-255> – Specify the table ID from 0 - 255.

`service show mint [adopted-devices {on <DEVICE-NAME>}|ports]`

show	Displays running system statistics based on the parameters passed
mint	Displays MiNT protocol details
adopted-devices on <DEVICE-NAME>	Displays adopted devices status in dpd2 • on <DEVICE-NAME> – Optional. Displays MiNT protocol details for a specified device. If no device is specified, the system displays information for the logged device. • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.
ports	Displays MiNT ports used by various services and features

`service show pm {history} {(on <DEVICE-NAME>)}`

show	Displays running system statistics based on the parameters passed
pm	Displays the *Process Monitor* (PM) controlled process details
history	Optional. Displays process change history (the time at which the change was implemented, and the events that triggered the change)
on <DEVICE-NAME>	Optional. Displays process change history for a specified device. If no device is specified, the system displays information for the logged device. • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

	`service show rf-domain-manager diag {<MAC/HOSTNAME>} {(on <DEVICE-OR-DOMAIN-NAME>)}`
show	Displays running system statistics based on the parameters passed
rf-domain-manager	Displays RF Domain manager information
diag	Displays RF Domain manager related diagnostics statistics
<MAC/HOSTNAME>	Optional. Specify the MAC address or hostname of the RF Domain manager.
on <DEVICE-OR-DOMAIN-NAME>	Optional. Displays diagnostics statistics on a specified device or domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

	`service show sites`
show	Displays running system statistics based on the parameters passed
sites	Displays NOC sites related information

	`service show virtual-machine-history {on <DEVICE-NAME>}`
show virtual-machine-history	Displays virtual machine history based on the parameters passed This command is applicable only to the Brocade Mobility RFS9510 series service platforms. It is also available on the Privilege Executable Mode of these devices.
on <DEVICE-NAME>	on <DEVICE-NAME> – Optional. Displays virtual machine history on a specified device. If no device is specified, the system displays information for the logged device. • <DEVICE-NAME> – Specify the name of the service platform.

	`service show wireless [aaa-stats|credential-cache|dns-cache|vlan-usage] {on <DEVICE-NAME>}`
show	Displays running system statistics based on the parameters passed
wireless	Displays WLAN statistics (WLAN AAA policy, configuration parameters, VLAN usage etc.)
aaa-stats	Displays AAA policy statistics
credential-cache	Displays clients cached credentials statistics (VLAN, keys etc.)
dns-cache	Displays cache of resolved names of servers related to wireless networking
vlan-usage	Displays VLAN statistics across WLANs
on <DEVICE-NAME>	The following keywords are common to all of the above: • on <DEVICE-NAME> – Optional. Displays running system statistics on a specified device. If no device is specified, the system displays information for the logged device. • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

	`service show wireless [client|meshpoint neighbor] proc [info|stats] {<MAC>} {(on <DEVICE-OR-DOMAIN-NAME)}`
show	Displays running system statistics based on the parameters passed
wireless	Displays WLAN statistics (WLAN AAA policy, configuration parameters, VLAN usage etc.)
client	Displays WLAN client statistics
meshpoint neighbor	Displays meshpoint related proc entries
proc	The following keyword is common to client and meshpoint neighbor parameters: • proc – Displays dataplane proc entries based on the parameter selected **NOTE:** These proc entries provide statistics on each wireless client on the WLAN. **NOTE:** For the meshpoint parameter, it displays proc entries about neighbors.

info	This parameter is common to client and meshpoint neighbor parameters. Displays information for a specified wireless client or neighbor
stats	This parameter is common to client and meshpoint neighbor parameters. Displays information for a specified wireless client or neighbor
<MAC>	Displays information for a specified wireless client or neighbor
on <DEVICE-OR-DOMAIN-NAME>	This parameter is common to client and meshpoint neighbor parameters. Displays information for a specified wireless client or neighbor.

`service show wireless reference dot11 [frame|mcs-rates|reason-codes|status-codes]`

show	Displays running system statistics based on the parameters passed
wireless	Displays WLAN statistics (WLAN AAA policy, configuration parameters, VLAN usage etc.)
reference	Displays look up reference information related to standards, protocols etc.
dot11	Displays 802.11 standard related information, such as frame structure, MCS rates etc.
frame	Displays 802.11 frame structure
mcs-rates	Displays MCS rate information
reason-codes	Displays 802.11 reason codes (for deauthentication, disassociation etc.)
status-codes	Displays 802.11 status codes (for association response etc.

`service show wireless reference dot11 handshake {wpa-wpa2-enterprise|wpa-wpa2-personal}`

show	Displays running system statistics based on the parameters passed
wireless	Displays WLAN statistics (WLAN AAA policy, configuration parameters, VLAN usage etc.)
reference	Displays look up reference information related to standards, protocols etc.
dot11	Displays 802.11 standard related information, such as frame structure, MCS rates etc.
handshake	Displays a flow diagram of 802.11 handshakes
wpa-wpa2-enterprise	Optional. Displays a WPA/WPA2 enterprise handshake (TKIP/CCMP with 802.1x authentication)
wpa-wpa2-personal	Optional. Displays a WPA/WPA2 personal handshake (TKIP/CCMP with pre-shared keys)

`service show wireless stats-client diag {<MAC/HOSTNAME>} {(on <DEVICE-OR-DOMAIN-NAME)}`

show	Displays running system statistics based on the parameters passed
wireless	Displays WLAN statistics (WLAN AAA policy, configuration parameters, VLAN usage etc.)
stats-client	Displays managed AP statistics
<MAC/HOSTNAME>	Optional. Specify the MAC address or hostname of the AP.
on <DEVICE-OR-DOMAIN-NAME>	Optional. Displays statistics on a specified AP, or all APs on a specified domain. • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

`service smart-rf clear-config {<MAC>|<DEVICE-NAME>|on <DOMAIN-NAME>}`

smart-rf	Enables Smart RF management
clear-config	Clears WLAN Smart RF configuration on a specified device or on all devices

<MAC>	Optional. Clears WLAN Smart RF configuration on a device identified by its MAC address. Specify the device's MAC address in the AA-BB-CC-DD-EE-FF format.
<DEVICE-NAME>	Optional. Clears WLAN Smart RF configuration on a device identified by its hostname. Specify the device's hostname.
on <DOMAIN-NAME>	Optional. Clears WLAN Smart RF configuration on all devices in a specified RF Domain • <DOMAIN-NAME> – Specify the RF Domain name.

```
service smart-rf [clear-history|interactive-calibration|run-calibration|
save-config|stop-calibration] {on <DOMAIN-NAME>}
```

smart-rf	Enables Smart RF management
clear-history	Clears WLAN Smart RF history on all devices
interactive-calibration	Enables an interactive Smart RF calibration
run-calibration	Starts a new Smart RF calibration process
save-config	Saves the Smart RF configuration on all devices, and also saves the history on the RF Domain Manager
stop-calibration	Stops an in-progress Smart RF calibration
on <DOMAIN-NAME>	Optional. Clears WLAN Smart RF configuration on all devices in a specified RF Domain • <DOMAIN-NAME> – Specify the RF Domain name.

```
service smart-rf interactive-calibration-result
[discard|replace-current-config|
write-to-configuration] {on <DOMAIN-NAME>}
```

smart-rf	Enables Smart RF management
interactive-calibration-result	Displays interactive Smart RF calibration results
discard	Discards interactive Smart RF calibration results
replace-current-config	Replaces current radio configuration
write-to-configuration	Writes and saves radio settings to configuration
on <DOMAIN-NAME>	Optional. Displays interactive Smart RF calibration results on a specified RF Domain • <DOMAIN-NAME> – Specify the RF Domain name.

```
service ssm dump-core-snapshot
```

ssm dump-core-snapshot	Triggers a debug core dump of the SSM module

```
service ssm trace pattern <WORD> {on <DEVICE-NAME>}
```

ssm trace	Displays the SSM module trace based on parameters passed
pattern <WORD>	Configures the pattern to match • <WORD> – Specify the pattern to match.
on <DEVICE-NAME>	Optional. Displays the SSM module trace on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
service wireless client beacon-request <MAC> mode [active|passive|table]
ssid [<SSID>|any] channel-report [<CHANNEL-LIST>|none] {on <DEVICE-NAME>}
```

wireless client beacon-requests	Sends beacon measurement requests to a wireless client
<MAC>	Specify the wireless client's MAC address.

mode [active|passive|table]	Specifies the beacon measurement mode. The following modes are available: • Active – Requests beacon measurements in the active mode • Passive – Requests beacon measurements in the passive mode • Table – Requests beacon measurements in the table mode
ssid [<SSID>|any]	Specifies if the measurements have to be made for a specified SSID or for any SSID • <SSID> – Requests beacon measurement for a specified SSID • any – Requests beacon measurement for any SSID
channel-report [<CHANNEL-LIST>| none]	Configures channel report in the request. The request can include a list of channels or can apply to all channels. • <CHANNEL-LIST> – Request includes a list of channels. The client has to send beacon measurements only for those channels included in the request • none – Request applies to all channels
on <DEVICE-NAME>	Optional. Sends requests on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`service wireless client quiet-element [start|stop]`

wireless client quiet-element	Enables/disables the quite-element information in beacons sent to wireless clients
start	Enables the quite-element information in beacons sent to wireless clients. This is the interval for which all wireless clients are to remain quiet.
stop	Disables the quite-element information in beacons sent to wireless clients. Once disabled, this information is no longer included in beacons.

`service wireless client trigger-bss-transition <MAC> url <URL> {on <DEVICE-OR-DOMAIN-NAME>}`

wireless client trigger-bss-transition	Sends a 80211v-Wireless Network Management BSS transition request to a client
<MAC>	Specifies the wireless client's MAC address
url <URL>	Specifies session termination URL
on <DEVICE-OR-DOMAIN-NAME>	Optional. Sends request on a specified device • <DEVICE-OR_DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

`service wireless dump-core-snapshot`

wireless client dump-core-snapshot	Triggers a debug core-dump of the wireless module

`service wireless meshpoint zl <MESHPOINT-NAME> [on <DEVICE-NAME>] {<ARGS>}`

service wireless meshpoint	Runs zonal level commands for a meshpoint
zl	Runs zonal commands
<MESHPOINT-NAME>	Runs zonal commands for the meshpoint identified by the <MESHPOINT-NAME> keyword
on <DEVICE-NAME>	Runs zonal commands for the specified meshpoint on a specified AP, wireless controller, or service platform
<ARGS>	Optional. Specifies the zonal arguments

`service wireless qos delete-tspec <MAC> tid <0-7>`

wireless qos delete-tspec	Sends a delete TSPEC request to a wireless client
<MAC>	Specify the MAC address of the wireless client.
tid <0-7>	Deletes the *Traffic Identifier* (TID) • <0-7> – Select the TID from 0 - 7.

`service wireless trace pattern <WORD> {on <DEVICE-NAME>}`

wireless trace	Displays the wireless module trace based on parameters passed
pattern <WORD>	Configures the pattern to match • <WORD> – Specify the pattern to match.
on <DEVICE-NAME>	Optional. Displays the wireless module trace on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`service wireless wips clear-client-blacklist [all|mac <MAC>]`

wireless wips	Enables management of WIPS parameters
clear-client-blacklist [all|mac <MAC>]	Removes a specified client or all clients from the blacklist • all – Removes all clients from the blacklist • mac <MAC> – Removes a specified client form the blacklist • <MAC> – Specify the wireless client's MAC address.

`service wireless wips clear-event-history {on <DEVICE-OR-DOMAIN-NAME}`

wireless wips	Enables WIPS management
clear-event-history	Clears event history
on <DEVICE-OR-DOMAIN-NAME>	Optional. Clears event history on a device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

Syntax: (Privilege Exec Mode)

NOTE
The "service" command of the Priv Exec Mode is the same as the service command in the User Exec Mode. There a few modifications that have been documented in this section. For the syntax and parameters of the other commands refer to the *(User Exec Mode)* syntax and *(User Exec Mode)* parameters sections of this chapter.

service

```
service [advanced-wips|block-adopter-config-updates|clear|

cli-tables-skin|cluster|copy|delete|delete-offline-aps|force-send-config|

force-update-vm-stats|load-balancing|locator|mint|pktcap|pm|radio|radius|

request-full-config-from-adopter|set|show|signal|smart-rf|ssm|start-shell|
          trace|wireless]

service copy tech-support [<FILE>|<URL>]

service clear crash-info {on <DEVICE-NAME>}
```

```
service delete sessions <SESSION-COOKIES>

service mint [clear|debug-log|expire|flood]
service mint [clear [lsp-db|mlcp]|debug-log [flash-and-syslog|flash-only]|
          expire [lsp|spf]|flood [csnp|lsp]]

service pktcap on
[bridge|deny|drop|ext-vlan|interface|radio|rim|router|vpn|wireless]
service pktcap on [bridge|deny|drop|ext-vlan|rim|router|vpn|wireless]
          {(acl-name <ACL>,count <1-1000000>,direction
[any|inbound|outbound],filter <LINE>,
          hex,rate <1-100>,snap <1-2048>,tcpdump,verbose,write [file|url|tzsp
[<IP/TZSP-
          HOSTNAME>])}
service pktcap on interface [<INTERFACE-NAME>|ge <1-4>|me1|port-channel <1-2>|
          pppoe1|vlan <1-4094>|wwan1] {(acl-name <ACL>,count <1-1000000>,
          direction [any|inbound|outbound],filter <LINE>,hex,rate <1-100>,
          snap <1-2048>,tcpdump,verbose,write [file|url|tzsp
[<IP/TZSP-HOSTNAME>])}
service pktcap on radio [<1-1024>|all] {(acl-name <ACL>,count <1-1000000>,
          direction [any|inbound|outbound],filter <LINE>,hex,promiscuous,rate
<1-100>,
          snap <1-2048>,tcpdump,verbose,write [file|url|tzsp
[<IP/TZSP-HOSTNAME>])}

service pm stop {on <DEVICE-NAME>}

service show last-passwd

service signal [abort <PROCESS-NAME>|kill <PROCESS-NAME>]

service start-shell

service trace <PROCESS-NAME> {summary}
```

Parameters (Privilege Exec Mode)

service

```
service copy tech-support [<FILE>|<URL>]
```

copy tech-support	Copies files for technical support • tech-support – Copies extensive system information useful for troubleshooting
<FILE>	Specify the file name and location using one of the following formats: cf:/path/file usb1:/path/file usb2:/path/file
<URL>	Specify the file location in one of the following formats: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>:<passwd>@<hostname|IP>[:port]>/path/file

```
service clear crash-info {on <DEVICE-NAME>}
```

clear crash-info	Clears all crash files
on <DEVICE-NAME>	Optional. Clears crash files on a specified device. These crash files are core, panic, and AP dump • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`service delete sessions <SESSION-COOKIES>`

delete sessions <SESSION-COOKIES>	Deletes session cookies • <SESSION-COOKIES> – Provide a list of cookies to delete.

`service mint [clear [lsp-dp|mlcp]|debug-log [flash-and-syslog|flash-only]| expire [lsp|spf]|flood [csnp|lsp]]`

mint	Enables MiNT protocol management (clears LSP database, enables debug logging, enables running silence etc.)
clear [lsp-dp|mlcp]	Clears LSP database and *MiNT Link Control Protocol* (MLCP) links • lsp-dp – Clears MiNT *Label Switched Path* (LSP) database • mlcp – Clears MLCP links
debug-log [flash-and-syslog| flash-only]	Enables debug message logging • flash-and-syslog – Logs debug messages to the flash and syslog files • flash-only – Logs debug messages to the flash file only
expire [lsp|spf]	Forces expiration of LSP and recalculation of *Shortest Path First* (SPF) • lsp – Forces expiration of LSP • spf – Forces recalculation of SPF
flood [csnp|lsp]	Floods control packets • csnp – Floods our *Complete Sequence Number Packets* (CSNP) • lsp – Floods our LSP

`service pm stop {on <DEVICE-NAME>}`

pm	Stops the *Process Monitor* (PM)
stops	Stops the PM from monitoring all daemons
on <DEVICE-NAME>	Optional. Stops the PM on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`service pktcap on [bridge|deny|drop|ext-vlan|rim|router|vpn|wireless] {(acl-name <ACL>,count <1-1000000>,direction [any|inbound|outbound],filter,hex, rate <1-100>,snap <1-2048>,tcpdump,verbose,write [file|url|tzsp <IP/TZSP-HOSTNAME>])}`

pktcap on	Captures data packets crossing at a specified location • on – Defines the packet capture location
bridge	Captures packets transiting through the Ethernet bridge
deny	Captures packets denied by an *Access Control List* (ACL)
drop	Captures packets at the drop locations
ext-vlan	Captures packets forwarded to or from an extended VLAN
rim	Captures packets at the *Radio Interface Module* (RIM)
router	Captures packets transiting through an IP router
vpn	Captures packets forwarded to or from a VPN link
wireless	Captures packets forwarded to or from a wireless device
acl-name <ACL>	Optional. Specify the ACL that matches the acl-name for the 'deny' location
count <1-1000000>	Optional. Limits the captured packet count. Specify a value from 1 -1000000.
direction [any|inbound|outbound]	Optional. Changes the packet direction with respect to a device. The direction can be set as any, inbound, or outbound.

filter [<LINE>|arp|capwap|cdp|dot11|dropreason|dst|ether|host|icmp|igmp|ip|ipv6|l2|l3|l4|lldp|mint|net|not|port|priority|radio|src|tcp|udp|vlan|wlan]	Optional. Filters packets based on the option selected (must be used as a last option) The filter options are: • <LINE> – Defines user defined packet capture filter • arp – Matches ARP packets • capwap – Matches CAPWAP packets • cdp – Matches CDP packets • dot11 – Matches 802.11 packets • dropreason – Matches packet drop reason • dst – Matches IP destination • ether – Matches Ethernet packets • host – Matches host destination • icmp – Matches ICMP packets • igmp – Matches IGMP packets • ip – Matches IPV4 packets • ipv6 – Matches IPV6 packets • l2 – Matches L2 header • l3 – Matches L3 header • l4 – Matches L4 header • lldp – Matches LLDP packets • mint – Matches MiNT packets • net – Matches IP in subnet • not – Filters out any packet that matches the filter criteria (For example, if not TCP is used, all tcp packets are filtered out) • port – Matches TCP or UDP port • priority – Matches packet priority • radio – Matches radio • src – Matches IP source • stp – Matches STP packets • tcp – Matches TCP packets • udp – Matches UDP packets • vlan – Matches VLAN • wlan – Matches WLAN
hex	Optional. Provides binary output of the captured packets
rate <1-100>	Optional. Specifies the packet capture rate • <1-100> – Specify a value from 1 - 100 seconds.
snap <1-2048>	Optional. Captures the data length • <1-2048> – Specify a value from 1 - 2048 characters.
tcpdump	Optional. Decodes tcpdump. The tcpdump analyzes network behavior, performance, and infrastructure. It also analyzes applications that generate or receive traffic.
verbose	Optional. Displays full packet body
write	Captures packets to a specified file. Provide the file name and location in the following format: FILE – flash:/path/file cf:/path/file usb1:/path/file usb2:/path/file vram:startup-config URL – tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file tzsp – *Tazman Sniffer Protocol* (TZSP) host. Specify the TZSP host's IP address or hostname.

	`service pktcap on radio [<1-1024>|all] {(acl-name <ACL>,count <1-1000000>,direction [any|inbound|outbound],filter <LINE>,hex,promiscuous,rate <1-100>,snap <1-2048>, tcpdump,verbose,write [file|url|tzsp <IP/TZSP-HOSTNAME>])}`
pktcap on radio	Captures data packets on a radio (802.11)
<1-1024>	Captures data packets on a specified radio • <1-1024> – specify the radio index from 1 - 1024.
all	Captures data packets on all radios
acl-name <ACL>	Optional. Specify the ACL that matches the ACL name for the 'deny' location
count <1-1000000>	Optional. Sets a specified number of packets to capture • <1-1000000> – Specify a value from 1 - 1000000.
direction [any|inbound|outbound]	Optional. Changes the packet direction with respect to a device. The direction can be set as any, inbound, or outbound.
filter <LINE>	Optional. Filters packets based on the option selected (must be used as a last option) • <LINE> – Define a packet capture filter or select any one of the available options.
hex	Optional. Provides binary output of the captured packets
rate <1-100>	Optional. Specifies the packet capture rate • <1-100> – Specify a value from 1 - 100 seconds.
snap <1-2048>	Optional. Captures the data length • <1-2048> – Specify a value from 1 - 2048 characters.
tcpdump	Optional. Decodes the TCP dump
verbose	Optional. Provides verbose output
write	Captures packets to a specified file. Provide the file name and location in the following format: FILE – flash:/path/file cf:/path/file usb1:/path/file usb2:/path/file nvram:startup-config URL – tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file tzsp – The TZSP host. Specify the TZSP host's IP address or hostname.
	`service pktcap on interface [<INTERFACE>|ge <1-4>|me|port-channel <1-2>|vlan <1-4094] {(acl-name <ACL>,count <1-1000000>,direction [any|inbound|outbound],filter <LINE>,hex,rate <1-100>,snap <1-2048>,tcpdump,verbose,write [file|url|tzsp <IP/TZSP-HOSTNAME>])}`
pktcap on	Captures data packets at a specified interface • on – Specify the capture location.
interface [<INTERFACE>| ge <1-4>|me1| port-channel <1-2>| vlan <1-4094>]	Captures packets at a specified interface. The options are: • <INTERFACE> – Specify the interface name. • ge <1-4> – Selects a GigabitEthernet interface index from 1 - 4 • me1 – Selects the FastEthernet interface • port-channel <1-2> – Selects a port-channel interface index from 1- 2 • vlan <1-4094> – Selects a VLAN ID from 1 - 4094
acl-name <ACL>	Optional. Specify the ACL that matches the ACL name for the 'deny' location
count <1-1000000>	Optional. Sets a specified number of packets to capture • <1-1000000> – Specify a value from 1 - 1000000.

direction [any|inbound|outbound]	Optional. Changes the packet direction with respect to a device. The direction can be set as any, inbound, or outbound.
filter <LINE>	Optional. Filters packets based on the option selected (must be used as a last option) • <LINE> – Define a packet capture filter or select any one of the available options.
hex	Optional. Provides binary output of the captured packets
rate <1-100>	Optional. Specifies the packet capture rate • <1-100> – Specify a value from 1 - 100 seconds.
snap <1-2048>	Optional. Captures the data length • <1-2048> – Specify a value from 1 - 2048 characters.
tcpdump	Optional. Decodes the TCP dump
verbose	Optional. Provides verbose output
write	Captures packets to a specified file. Provide the file name and location in the following format: FILE – flash:/path/file cf:/path/file usb1:/path/file usb2:/path/file nvram:startup-config URL – tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file tzsp – The TZSP host. Specify the TZSP host's IP address or hostname.

`service show last-passwd`

show	Displays running system statistics based on the parameters passed
last-passwd	Displays the last password used to enter shell

`service signal [abort <PROCESS-NAME>|kill <PROCESS-NAME>]`

signal	Sends a signal to a process • tech-support – Copies extensive system information useful for troubleshooting
abort	Sends an abort signal to a process, and forces it to dump to core • <PROCESS-NAME> – Specify the process name.
kill	Sends a kill signal to a process, and forces it to terminate without a core • <PROCESS-NAME> – Specify the process name.

`service start-shell`

start-shell	Provides shell access

`service trace <PROCESS-NAME> {summary}`

trace	Traces a process for system calls and signals
<PROCESS-NAME>	Specifies the process name
summary	Optional. Generates summary report of the specified process

Syntax: (Privilege Exec Mode: Brocade Mobility RFS9510)

service

The following service commands are specific to the Brocade Mobility RFS9510 series service platforms:

```
service analytics
[clear-data|get-last-detailed-status|migrate|nfsserver|primary|
          restart|secondary|start|start-detailed-status|status|stop]

service analytics [clear-data|get-last-detailed-status|migrate|restart|start|
          start-detailed-status|status|stop]

service analytics nfsserver [<IP>|<HOST-NAME>]

service analytics primary [<IP>|<HOST-NAME>]

service analytics secondary [<IP>|<HOST-NAME>]

service copy [<URL>|analytics-support|mac-user-db|tech-support]


service copy <URL>

service copy analytics-support [<FILE>|<URL>]

service copy mac-user-db <URl>
```

Parameters (Privilege Exec Mode: Brocade Mobility RFS9510)

service

```
service analytics
[clear-data|get-last-detailed-status|migrate|restart|start|start-detailed-sta
tus|status|stop]
```

service analytics	Provides analytics services The analytics feature is a separately licensed feature available only on the Brocade Mobility RFS9510 model (NOC) service platforms and their managed controllers, service platforms, and access points. When enabled, this feature provides granular and robust analytic reporting for a controller managed (Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000) network. Using analytics, data is collected at administrator defined intervals. Use *nfsserver* command to configure the *Network File Server* (NFS) To configure the license string for the hotspot analytics feature, see *license*.
clear-data	Clears analytics data
get-last-detailed-status	Retrieves the last detailed status (Hadoop/Hbase status and database sync status) In case no status is returned, retry the command after an interval, as the command issued to determine the detailed status (start-detail-status) might not have completed.
migrate	Deletes current analytics data and migrated 5.4.X analytics data
restart	Restarts analytics services
start	Starts analytics services
start-detailed-status	Initiates a detailed status computation
stop	Stops analytics services

```
service analytics nfsserver [<IP>|<HOST-NAME>]
```

service analytics	Provides analytics services
nfsserver [<IP>|<HOST-NAME>]	Configures the analytics NFS server. Use one of the following options to identify the NFS server: • <IP> – Specifies the NFS server's IP address • <HOST-NAME> – Specifies the NFS server's hostname

`service analytics primary [<IP>|<HOST-NAME>]`

service analytics	Provides analytics services
primary [<IP>|<HOST-NAME>]	Configures the analytics primary server. Use one of the following options to identify the primary server: • <IP> – Specifies the primary server's IP address • <HOST-NAME> – Specifies the primary server's hostname

`service analytics secondary [<IP>|<HOST-NAME>]`

service analytics	Provides analytics services
secondary [<IP>|<HOST-NAME>]	Configures the analytics primary server. Use one of the following options to identify the secondary server: • <IP> – Specifies the secondary server's IP address • <HOST-NAME> – Specifies the secondary server's hostname

`service copy analytics-support [<FILE>|<URL>]`

cop analytics-support	Enables copying of analytics information to a specified. Use one of the following options to specify the file: This information is useful to troubleshoot issues by the Technical Support team.
<FILE>	Specify the file name and location using one of the following formats: usb1:/path/file usb2:/path/file
<URL>	Specify the file location in one of the following formats: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>:<passwd>@<hostname|IP>[:port]>/path/file

`service copy <URL>`

copy <URL>	Imports files from a specified location. Use one of the following options to specify the file to copy and the location: URL – tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file

`service copy mac-user-db <URL>`

copy mac-user-db	Exports MAC user database file (in the *comma-separated values* (CSV) format) to a specified location. Use one of the following options to specify the file to copy and the location: URL – tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file

Usage Guidelines:

The Brocade Mobility RFS9510 model service platforms (NOC) provide granular and robust analytic reporting for a Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000 device managed network. The data analyzed is collected at intervals specified by the administrator.

To enable data analytics, procure and apply a separate hot spare analytics license at the NOC. The license restricts the number of access point streams processed at the NOC or forwarded to partner systems for further processing. The analytics feature can be turned on at select APs by enabling them in configuration. This way the customer can enable analytics on a select set of APs and not the entire system as long as the number of APs on which it is enabled is less than or equal to the total number of AP analytics licenses available at the NOC controller.

In an NOC managed network, the analytics engine parses and processes Smart RF events as they are received. The analytics engine parses the new channel and power information from the Smart RF event, as opposed to retrieving the event from the devices themselves.

Syntax: (Global Config Mode)

```
service

service [set|show cli]
service set [command-history <10-300>|upgrade-history <10-100>|reboot-history
          <10-100>|virtual-machine-history <10-200>] {on <DEVICE-NAME>}
```

Parameters (Global Config Mode)

```
service set [command-history <10-300>|upgrade-history <10-100>|reboot-history
<10-100>] {on <DEVICE-NAME>}
```

set	Sets the size of history files
command-history <10-300>	Sets the size of the command history file • <10-300> – Specify a value from 10 - 300. The default is 200.
upgrade-history <10-100>	Sets the size of the upgrade history file • <10-100> – Specify a value from 10 - 100. The default is 50.
reboot-history <10-100>	Sets the size of the reboot history file • <10-100> – Specify a value from 10 - 100. The default is 50.
virtual-machine-history <10-200>	Sets the size of the virtual-machine history file • <10-200> – Specify a value from 10 - 200. The default is 100. This command is applicable only to the Brocade Mobility RFS9510 series service platforms. Use the *no > service > set > virtual-machine-history > {on <DEVICE-NAME>}* to revert the history file size to 100.
on <DEVICE-NAME>	Optional. Sets the size of history files on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
service show cli
```

show cli	Displays running system configuration details • cli – Displays the CLI tree of the current mode

Example

```
rfs7000-37FABE>service cli-tables-skin stars

rfs7000-37FABE>service pktcap on interface vlan 2
Capturing up to 50 packets. Use Ctrl-C to abort.

rfs7000-37FABE>service show cli
User Exec mode:  +-do
+-help [help]
  +-show
    +-configuration-tree [help show configuration-tree]
  +-search
    +-WORD [help search WORD (|detailed|only-show|skip-show)]
      +-detailed [help search WORD (|detailed|only-show|skip-show)]
      +-only-show [help search WORD (|detailed|only-show|skip-show)]
      +-skip-show [help search WORD (|detailed|only-show|skip-show)]
+-show
  +-commands [show commands]
  +-running-config [show (running-config|session-config) (|include-factory)]
```

```
    +-include-factory [show (running-config|session-config)
(|include-factory)]
    +-interface [show running-config interface (|`WORD|ge <1-4>|me1|pc
<1-4>|vlan <1-4094>') (|include-factory)]
     +-WORD [show running-config interface (|`WORD|ge <1-4>|me1|pc <1-4>|vlan
<1-4094>') (|include-factory)]
       +-include-factory [show running-config interface (|`WORD|ge
<1-4>|me1|pc <1-4>|vlan <1-4094>') (|include-factory)]
      +-ge
        +-<1-4> [show running-config interface (|`WORD|ge <1-4>|me1|pc
<1-4>|vlan <1-4094>') (|include-factory)]
          +-include-factory [show running-config interface (|`WORD|ge
<1-4>|me1|pc <1-4>|vlan <1-4094>') (|includefactory)]
--More--
rfs7000-37FABE>

rfs7000-37FABE#service signal kill testp
Sending a kill signal to testp
rfs7000-37FABE#

rfs7000-37FABE#service signal abort testprocess
Sending an abort signal to testprocess
rfs7000-37FABE#

rfs7000-37FABE#service pm stop on rfs7000-37FABE
rfs7000-37FABE#

rfs7000-37FABE(config)#service show cli
Global Config mode:
+-help [help]
  +-search
    +-WORD [help search WORD (|detailed|only-show|skip-show)]
      +-detailed [help search WORD (|detailed|only-show|skip-show)]
      +-only-show [help search WORD (|detailed|only-show|skip-show)]
      +-skip-show [help search WORD (|detailed|only-show|skip-show)]
+-show
  +-commands [show commands]
  +-eval
    +-LINE [show eval LINE]
  +-debugging [show debugging (|(on DEVICE-OR-DOMAIN-NAME))]
    +-cfgd [show debugging cfgd]
    +-on
      +-DEVICE-OR-DOMAIN-NAME [show debugging (|(on DEVICE-OR-DOMAIN-NAME))]
    +-wireless [show debugging wireless (|(on DEVICE-OR-DOMAIN-NAME))]
      +-on
        +-DEVICE-OR-DOMAIN-NAME [show debugging wireless (|(on
DEVICE-OR-DOMAIN-NAME))]
    +-voice [show debugging voice (|(on DEVICE-OR-DOMAIN-NAME))]
      +-on
        +-DEVICE-OR-DOMAIN-NAME [show debugging voice (|(on
DEVICE-OR-DOMAIN-NAME))]
 --More--
rfs7000-37FABE(config)#

rfs4000-229D58>service show command-history on rfs4000-229D58
Configured size of command history is 200

  Date & Time          User      Location           Command
======================================================================
```

```
Feb 15 14:44:19 2013   admin     192.168.100.225 46      clock set 14:45:30 15
Feb 2013
Feb 15 14:41:10 2013   admin     192.168.100.225 46       clear event-history
Feb 15 14:38:28 2013   admin     192.168.100.225 46       boot system primary
Feb 15 14:35:54 2013   admin     192.168.100.225 46       boot system secondary
Jan 31 01:07:59 2013   admin     192.168.100.225 46      clock set 14:25:35 15
Feb 2013
Jan 31 01:07:47 2013   admin     192.168.100.225 46      clock set 14:25:35 15
02 2013
Jan 31 01:05:58 2013   admin     192.168.100.225 46
captive-portal-page-upload cancel-upload 00-04-96-4A-A7-08
Jan 31 01:04:45 2013   admin     192.168.100.225 46
captive-portal-page-upload cancel-upload on rf-domain test
Jan 31 01:02:56 2013   admin     192.168.100.225 46
captive-portal-page-upload cancel-upload on rf-domain default
Jan 31 01:01:22 2013   admin     192.168.100.225 46
captive-portal-page-upload test1  00-04-96-4A-A7-08 upload-time
03/01/2013-12:30
Jan 31 01:01:03 2013   admin     192.168.100.225 46
captive-portal-page-upload test 00-04-96-4A-A7-08 upload-time 03/01/2013-12:30
Jan 31 00:59:57 2013   admin     192.168.100.225 46
captive-portal-page-upload cancel-upload all
Jan 31 00:59:23 2013   admin     192.168.100.225 46
captive-portal-page-upload test all
Jan 31 00:58:40 2013   admin     192.168.100.225 46       exit
--More--
rfs4000-229D58>

rfs7000-37FABE>service show diag stats on rfs7000-37FABE

fan 1 current speed: 6660 min_speed: 2000 hysteresis: 250
fan 2 current speed: 6720 min_speed: 2000 hysteresis: 250
fan 3 current speed: 6540 min_speed: 2000 hysteresis: 250

Sensor 1 Temperature 32.0 C
Sensor 2 Temperature 58.0 C
Sensor 3 Temperature 29.0 C
Sensor 4 Temperature 28.0 C
Sensor 5 Temperature 26.0 C
Sensor 6 Temperature 28.0 C
rfs7000-37FABE>

rfs7000-37FABE>service show info on rfs7000-37FABE
7.9M out of 8.0M available for logs.
32.9M out of 34.0M available for history.
81.9M out of 84.0M available for crashinfo.

List of Files:

anald.log                              1.3K    Apr 4  10:48
cfgd.log                               9.7K    Apr 4  14:38
dpd2.log                               21.4K   Apr 4  10:48
messages.log                           0       Apr 4  10:46
startup.log                            9.5K    Apr 4  10:48
upgrade.log                            1.6K    Apr 4  10:50
vlan-usage.log                         0       Apr 4  14:32
command.history                        1.6K    Apr 4  14:37
reboot.history                         2.1K    Apr 4  10:46
ugrade.history                         522     Apr 4  10:45
```

```
Please export these files or delete them for more space.

rfs7000-37FABE>

rfs4000-229D58>service show upgrade-history on rfs4000-229D58
Configured size of upgrade history is 50

  Date & Time            Old Version     New Version     Status
=========================================================================
Jan 16 22:28:19 2013 5.5.0.0-017D 5.5.0.0-018D Successful
Jan 13 22:51:38 2013 5.5.0.0-015D 5.5.0.0-017D Successful
Dec 04 01:25:18 2012 5.5.0.0-011D 5.5.0.0-015D Successful
Oct 04 22:25:03 2012 5.4.2.0-012D 5.5.0.0-011D Successful
rfs4000-229D58>

rfs4000-229D58>service show xpath-history
-------------------------------------------------------------------------------
-------------------------------------------------------------
     DATE&TIME       USER                        XPATH
DURATION(MS)
-------------------------------------------------------------------------------
-------------------------------------------------------------
  Fri Feb 15 15:02:59 2013   system
/Mobility-stats/device/00-23-68-22-9D-58/upgrade-history
10
  Fri Feb 15 15:01:12 2013   system
/Mobility-stats/device/00-23-68-22-9D-58/command-history
15
  Fri Feb 15 14:59:21 2013   system
/Mobility-stats/device/00-23-68-22-9D-58/event-history
5
  Fri Feb 15 14:45:43 2013   system
/Mobility-stats/device/00-23-68-22-9D-58/system/clock
6
  Fri Feb 15 14:44:19 2013   system
/Mobility-stats/device/00-23-68-22-9D-58/_actions/clock_set
70096
  Fri Feb 15 14:42:51 2013   system
/Mobility-stats/device/00-23-68-22-9D-58/event-history
5
--More--
rfs4000-229D58>

rfs7000-37FABE>service show wireless config-internal
! Startup-Config-Playback Completed: Yes
no debug wireless
no country-code
!
wlan-qos-policy default
 no rate-limit wlan to-air
 no rate-limit wlan from-air
 no rate-limit client to-air
 no rate-limit client from-air
!
wlan wlan1
 ssid wlan1
 vlan 1
 qos-policy default
 encryption-type none
 authentication-type none
```

```
 no accounting radius
 no accounting syslog
rfs7000-37FABE>

System Information:

Free RAM:  68.0% (169 of 249)  Min: 10.0%
File Descriptors: free: 24198 used: 960 max: 25500
CPU load averages: 1 min: 0.0%  5 min: 0.0%  15 min: 0.0%

Kernel Buffers:
Size:      32    64   128   256   512    1k    2k    4k    8k   16k   32k   64k
128k
Usage:   2761  2965   927   201   549   107   141    25    68     0     1     2
0
Limit:  32768  8192  4096  4096  8192  8192 16384 16384  1024   512   256    64
64
rfs7000-37FABE#

rfs4000-229D58#show adoption history on br650-983278
-----------------------------------------------------------------------
       MAC     TYPE     EVENT      TIME_STAMP        REASON
-----------------------------------------------------------------------
00-23-68-22-9D-58   Brocade Mobility RFS4000    adopted  2013-02-21 11:37:37
N.A
-----------------------------------------------------------------------
rfs4000-229D58#

rfs4000-229D58#service clear adoption history on br650-983278

rfs4000-229D58#show adoption history on br650-983278
-----------------------------------------------------------------------
       MAC     TYPE     EVENT      TIME_STAMP        REASON
-----------------------------------------------------------------------

-----------------------------------------------------------------------
rfs4000-229D58#
```

show

Common Commands

Displays specified system component settings. There are a number of ways to invoke the show command:

- When invoked without any arguments, it displays information about the current context. If the current context contains instances, the show command (usually) displays a list of these instances.
- When invoked with the display parameter, it displays information about that component.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show <PARAMETER>
```

Parameters

None

Example

```
rfs7000-37FABE#show ?
  adoption                    Display information related to adoption to
                              wireless controller
  advanced-wips               Advanced WIPS
  boot                        Display boot configuration.
  captive-portal              Captive portal commands
  captive-portal-page-upload  Captive portal advanced page upload
  cdp                         Cisco Discovery Protocol
  clock                       Display system clock
  cluster                     Cluster Protocol
  commands                    Show command lists
  context                     Information about current context
  critical-resources          Critical Resources
  crypto                      Encryption related commands
  debug                       Debugging functions
  debugging                   Debugging functions
  device-upgrade              Device Upgrade
  dot1x                       802.1X
  environmental-sensor        Display Environmental Sensor Module status
  event-history               Display event history
  event-system-policy         Display event system policy
  file                        Display filesystem information
  firewall                    Wireless Firewall
  global                      Global-level information
  gre                         Show gre tunnel info
  interface                   Interface Configuration/Statistics commands
  ip                          Internet Protocol (IP)
  ip-access-list              IP ACL
  l2tpv3                      L2TPv3 information
  ldap-agent                  LDAP Agent Configuration
  licenses                    Show installed licenses and usage
  lldp                        Link Layer Discovery Protocol
  logging                     Show logging information
  mac-access-list             MAC Access list
  mac-address-table           Display MAC address table
  macauth                     MAC AUTH
  mint                        MiNT protocol
  ntp                         Network time protocol
  password-encryption         Pasword encryption
  power                       Show power over ethernet command
  pppoe-client                PPP Over Ethernet client
  privilege                   Show current privilege level
  reload                      Scheduled reload information
  remote-debug                Show details of remote debug sessions
  rf-domain-manager           Show RF Domain Manager selection details
  role                        Role based firewall
  route-maps                  Display Route Map Statistics
  rtls                        RTLS Statistics
  running-config              Current operating configuration
```

```
  session-changes            Configuration changes made in this session
  session-config             This session configuration
  sessions                   Display CLI sessions
  site-config-diff           Difference between site configuration on the NOC
                             and actual site configuration
  smart-rf                   Smart-RF Management Commands
  spanning-tree              Display spanning tree information
  startup-config             Startup configuration
  terminal                   Display terminal configuration parameters
  timezone                   The timezone
  upgrade-status             Display last image upgrade status
  version                    Display software & hardware version
  vrrp                       VRRP protocol
  what                       Perform global search
  wireless                   Wireless commands
  wwan                       Display wireless WAN Status

rfs7000-37FABE#
t
```

NOTE
For more information on the show command, see *Chapter 6, SHOW COMMANDS*.

write

Common Commands

Writes the system running configuration to memory or terminal

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
write [memory|terminal]
```

Parameters

```
write [memory|terminal]
```

memory	Writes to the *non-volatile* (NV) memory
terminal	Writes to the terminal

Example

```
rfs7000-37FABE>write memory
[OK]
rfs7000-37FABE>
```

Chapter

SHOW COMMANDS

6

Show commands display configuration settings or statistical information. Use this command to view the current running configuration as well as the start-up configuration. The show command also displays the current context's configuration.

This chapter describes the 'show' CLI commands used in the USER EXEC, PRIV EXEC, and GLOBAL CONFIG modes. Commands entered in either USER EXEC mode or PRIV EXEC mode are referred to as EXEC mode commands. If a user or privilege is not specified, the referenced command can be entered in either mode.

This chapter also describes the 'show' commands in the 'GLOBAL CONFIG' mode. The commands can be entered in all three modes, except commands like file, IP access list statistics, MAC access list statistics, and upgrade statistics, which cannot be entered in the USER EXEC mode.

show commands

Table 4 summarizes show commands.

TABLE 4 Show Commands

Command	Description	Reference
show	Displays settings for the specified system component	page 429
adoption	Displays information related to adoption	page 434
advanced-wips	Displays advanced *Wireless Intrusion Prevention System* (WIPS) settings	page 436
boot	Displays a device boot configuration	page 438
captive-portal	Displays WLAN hotspot functions	page 439
captive-portal-page-upload	Displays captive portal page related information	page 443
cdp	Displays a *Cisco Discovery Protocol* (CDP) neighbor table	page 444
clock	Displays the software system clock	page 445
cluster	Displays cluster commands	page 446
commands	Displays command list	page 447
context	Displays information about the current context	page 448
critical-resources	Displays critical resource information	page 449
crypto	Displays encryption mode information	page 450
device-upgrade	Displays device firmware upgradation information for devices adopted by a wireless controller or access point	page 453
dot1x	Displays dot1x information on interfaces	page 454
environmental-sensor	Displays environmental sensor's historical data (applicable only to Brocade Mobility 1240 Access Point)	page 456

TABLE 4 Show Commands

Command	Description	Reference
event-history	Displays event history	page 460
event-system-policy	Displays event system policy configuration information	page 461
file	Displays file system information	page 462
firewall	Displays wireless firewall information	page 463
global	Displays global information for network devices based on the parameters passed	page 466
gre	Displays GRE tunnel related information	page 468
interface	Displays interface status	page 468
ip	Displays IP related information	page 472
ip-access-list	Displays IP access list statistics	page 478
l2tpv3	Displays *Layer 2 Tunnel Protocol Version 3* (L2TPV3) information	page 479
ldap-agent	Displays an LDAP agent's join status (join status to a LDAP server domain)	page 481
licenses	Displays installed licenses and usage information	page 482
lldp	Displays *Link Layer Discovery Protocol* (LLDP) information	page 485
logging	Displays logging information	page 486
mac-access-list-stats	Displays MAC access list statistics	page 487
mac-address-table	Displays MAC address table entries	page 487
macauth	Displays details of wired ports that have MAC address-based authentication enabled	page 488
mint	Displays MiNT protocol configuration commands	page 489
ntp	Displays *Network Time Protocol* (NTP) information	page 492
password-encryption	Displays password encryption status	page 493
pppoe-client	Displays *Point to Point Protocol over Ethernet* (PPPoE) client information	page 493
privilege	Displays current privilege level information	page 494
reload	Displays scheduled reload information	page 495
rf-domain-manager	Displays RF Domain manager selection details	page 495
role	Displays role-based firewall information	page 496
route-maps	Display route map statistics	page 497
rtls	Displays *Real Time Location Service* (RTLS) statistics of access points	page 497
running-config	Displays configuration file contents	page 498
session-changes	Displays configuration changes made in this session	page 503
session-config	Displays a list of currently active open sessions on the device	page 503
sessions	Displays CLI sessions	page 504
site-config-diff	Displays the difference between site configuration available on NOC and the actual site configuration	page 505
smart-rf	Displays Smart RF management commands	page 506
spanning-tree	Displays spanning tree information	page 509
startup-config	Displays complete startup configuration script on the console	page 511

TABLE 4 Show Commands

Command	Description	Reference
terminal	Displays terminal configuration parameters	page 512
timezone	Displays timezone information for the system and managed devices	page 513
upgrade-status	Displays image upgrade status	page 513
version	Displays a device's software and hardware version	page 514
vrrp	Displays *Virtual Router Redundancy Protocol* (VRRP) protocol details	page 515
what	Displays details of a specified search phrase	page 516
wireless	Displays wireless configuration parameters	page 517
wwan	Displays the wireless WAN status	page 533
smart-cache	Displays details on the cached entry for a specific URL or all URLs	page 534

show

show commands

The show command displays following information:

- A device's current configuration
- A device's start-up configuration
- A device's current context configuration, such as profiles and policies

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show <PARAMETER>
```

Parameters

None

Example

The following examples list the *show* commands in the User Exec, Priv Exec, and Global Config modes:

GLOBAL CONFIG Mode

```
<DEVICE>(config)#show ?
  adoption                  Display information related to adoption to
                            wireless controller
  advanced-wips             Advanced WIPS
  boot                      Display boot configuration.
  captive-portal            Captive portal commands
```

```
captive-portal-page-upload  Captive portal advanced page upload
cdp                         Cisco Discovery Protocol
clock                       Display system clock
cluster                     Cluster Protocol
commands                    Show command lists
context                     Information about current context
critical-resources          Critical Resources
crypto                      Encryption related commands
debug                       Debugging functions
debugging                   Debugging functions
device-upgrade              Device Upgrade
dot1x                       802.1X
environmental-sensor        Display Environmental Sensor Module status
event-history               Display event history
event-system-policy         Display event system policy
file                        Display filesystem information
firewall                    Wireless Firewall
global                      Global-level information
gre                         Displays gre related information
interface                   Interface Configuration/Statistics commands
ip                          Internet Protocol (IP)
ip-access-list              IP ACL
l2tpv3                      L2TPv3 information
ldap-agent                  LDAP Agent Configuration
licenses                    Show installed licenses and usage
lldp                        Link Layer Discovery Protocol
logging                     Show logging information
mac-access-list             MAC ACL
mac-address-table           Display MAC address table
macauth                     MAC AUTH
mint                        MiNT protocol
mirroring                   Show mirroring sessions
ntp                         Network time protocol
password-encryption         Password encryption
power                       Show power over ethernet command
pppoe-client                PPP Over Ethernet client
privilege                   Show current privilege level
raid                        Show RAID status
reload                      Scheduled reload information
remote-debug                Show details of remote debug sessions
rf-domain-manager           Show RF Domain Manager selection details
role                        Role based firewall
route-maps                  Display Route Map Statistics
rtls                        RTLS Statistics
running-config              Current operating configuration
session-changes             Configuration changes made in this session
session-config              This session configuration
sessions                    Display CLI sessions
site-config-diff            Difference between site configuration on the NOC
                            and actual site configuration
slot                        Expansion slots stats
smart-cache                 Content caching
smart-rf                    Smart-RF Management Commands
spanning-tree               Display spanning tree information
startup-config              Startup configuration
terminal                    Display terminal configuration parameters
timezone                    The timezone
upgrade-status              Display last image upgrade status
version                     Display software & hardware version
virtual-machine             Virtual Machine
```

```
  vrrp                        VRRP protocol
  what                        Perform global search
  wireless                    Wireless commands
  wwan                        Display wireless WAN Status

<DEVICE>(config)#

rfs7000-37FABE(config)#show clock
2013-02-15 15:28:26 UTC
rfs7000-37FABE(config)#

PRIVILEGE EXEC Mode
<DEVICE>#show ?
  adoption                    Display information related to adoption to
                              wireless controller
  advanced-wips               Advanced WIPS
  boot                        Display boot configuration.
  captive-portal              Captive portal commands
  captive-portal-page-upload  Captive portal advanced page upload
  cdp                         Cisco Discovery Protocol
  clock                       Display system clock
  cluster                     Cluster Protocol
  commands                    Show command lists
  context                     Information about current context
  critical-resources          Critical Resources
  crypto                      Encryption related commands
  debug                       Debugging functions
  debugging                   Debugging functions
  device-upgrade              Device Upgrade
  dot1x                       802.1X
  environmental-sensor        Display Environmental Sensor Module status
  event-history               Display event history
  event-system-policy         Display event system policy
  file                        Display filesystem information
  firewall                    Wireless Firewall
  global                      Global-level information
  gre                         Negate a command or set its defaults
  interface                   Interface Configuration/Statistics commands
  ip                          Internet Protocol (IP)
  ip-access-list              IP ACL
  l2tpv3                      L2TPv3 information
  ldap-agent                  LDAP Agent Configuration
  licenses                    Show installed licenses and usage
  lldp                        Link Layer Discovery Protocol
  logging                     Show logging information
  mac-access-list             MAC ACL
  mac-address-table           Display MAC address table
  macauth                     MAC AUTH
  mint                        MiNT protocol
  mirroring                   Show mirroring sessions
  ntp                         Network time protocol
  password-encryption         Password encryption
  power                       Show power over ethernet command
  pppoe-client                PPP Over Ethernet client
  privilege                   Show current privilege level
  raid                        Show RAID status
  reload                      Scheduled reload information
  remote-debug                Show details of remote debug sessions
  rf-domain-manager           Show RF Domain Manager selection details
  role                        Role based firewall
```

```
  route-maps                  Display Route Map Statistics
  rtls                        RTLS Statistics
  running-config              Current operating configuration
  session-changes             Configuration changes made in this session
  session-config              This session configuration
  sessions                    Display CLI sessions
  site-config-diff            Difference between site configuration on the NOC
                              and actual site configuration
  slot                        Expansion slots stats
  smart-cache                 Content caching
  smart-rf                    Smart-RF Management Commands
  spanning-tree               Display spanning tree information
  startup-config              Startup configuration
  terminal                    Display terminal configuration parameters
  timezone                    The timezone
  upgrade-status              Display last image upgrade status
  version                     Display software & hardware version
  virtual-machine             Virtual Machine
  vrrp                        VRRP protocol
  what                        Perform global search
  wireless                    Wireless commands
  wwan                        Display wireless WAN Status

<DEVICE>#

rfs7000-37FABE#show terminal
Terminal Type: xterm
Length: 24     Width: 80
rfs7000-37FABE#

USER EXEC Mode
<DEVICE>>show ?
  adoption                    Display information related to adoption to
                              wireless controller
  advanced-wips               Advanced WIPS
  boot                        Display boot configuration
  captive-portal              Captive portal commands
  captive-portal-page-upload  Captive portal advanced page upload
  cdp                         Cisco Discovery Protocol
  clock                       Display system clock
  cluster                     Cluster Protocol
  commands                    Show command lists
  context                     Information about current context
  critical-resources          Critical Resources
  crypto                      Encryption related commands
  debug                       Debugging functions
  debugging                   Debugging functions
  device-upgrade              Device Upgrade
  dot1x                       802.1X
  environmental-sensor        Display Environmental Sensor Module status
  event-history               Display event history
  event-system-policy         Display event system policy
  firewall                    Wireless Firewall
  global                      Global-level information
  gre                         Negate a command or set its defaults
  interface                   Interface Configuration/Statistics commands
  ip                          Internet Protocol (IP)
  licenses                    Show installed licenses and usage
  lldp                        Link Layer Discovery Protocol
  logging                     Show logging information
```

```
  mac-address-table           Display MAC address table
  macauth                     MAC AUTH
  mint                        MiNT protocol
  mirroring                   Show mirroring sessions
  ntp                         Network time protocol
  password-encryption         Password encryption
  power                       Show power over ethernet command
  pppoe-client                PPP Over Ethernet client
  privilege                   Show current privilege level
  rf-domain-manager           Show RF Domain Manager selection details
  role                        Role based firewall
  route-maps                  Display Route Map Statistics
  rtls                        RTLS Statistics
  running-config              Current operating configuration
  session-changes             Configuration changes made in this session
  session-config              This session configuration
  sessions                    Display CLI sessions
  site-config-diff            Difference between site configuration on the NOC
                              and actual site configuration
  slot                        Expansion slots stats
  smart-rf                    Smart-RF Management Commands
  spanning-tree               Display spanning tree information
  startup-config              Startup configuration
  terminal                    Display terminal configuration parameters
  timezone                    The timezone
  version                     Display software & hardware version
  vrrp                        VRRP protocol
  what                        Perform global search
  wireless                    Wireless commands
  wwan                        Display wireless WAN Status

<DEVICE>>

rfs7000-37FABE(config)#show wireless br configured
------------------------------------------------------------------------------
----------
IDX         NAME                MAC              PROFILE       RF-DOMAIN
ADOPTED-BY
------------------------------------------------------------------------------
----------
  1    br7131-889EC4      00-15-70-88-9E-C4   default-br7131    default
un-adopted
5    br650-3481BC       5C-0E-8B-34-81-BC   default-br650     default
un-adopted
  6    br6511-08456A      5C-0E-8B-08-45-6A   default-br6511    default
un-adopted
8    br1220-7BF224      5C-0E-8B-7B-F2-24   default-br1220    default
un-adopted
11   br7131-99BFA8      00-23-68-99-BF-A8   default-br71xx    default
un-adopted
  12   br8132-BEF116      C4-01-FA-BE-F1-16   default-br81xx    default
un-adopted
------------------------------------------------------------------------------
----------
rfs7000-37FABE(config)#
```

The following *Show* commands are specific to the Brocade Mobility RFS9510 series service platforms:

```
nx9500-6C874D(config)#show virtual-machine configuration
------------------------------------------------------------------------------
---
         NAME              AUTOSTART           MEMORY(MB)            VCPUS
------------------------------------------------------------------------------
---
  Mobility                   -                   16384                -
  adsp                  start               16384                12
  team-cmt              start               1024                 1
------------------------------------------------------------------------------
---
nx9500-6C874D(config)#
```

adoption

show commands

Displays adoption related information, and is common to the User Exec, Priv Exec, and Global Config modes.

In an *hierarchically managed* (HM) network devices are deployed in two levels. The first level consists of the *Network Operations Center* (NOC) controllers. The second level consists of the site controllers that can be grouped to form clusters. The NOC controllers adopt and manage the site controllers. Access points within the network are adopted and managed by the site controllers. The adopted devices (access points and second-level controllers) are referred to as the adoptee. The devices adopting the adoptee are the 'adopters'.

Use this command to confirm if a device is an adoptee or an adopter. This command also allows you to determine the devices adopted by an adopter device.

NOTE
A NOC controller's capacity is equal to or higher than a site controller's capacity. The following devices can be deployed at NOC and sites:
- NOC controller – Brocade Mobility RFS6000, Brocade Mobility RFS7000, or Brocade Mobility RFS9510.
- Site controller – Brocade Mobility RFS7000, Brocade Mobility RFS6000, or Brocade Mobility RFS4000.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — , Brocade Mobility RFS9510

```
show adoption
[config-errors|controllers|history|info|log|offline|pending|status|
          timeline]

show adoption offline
show adoption config-errors <DEVICE-NAME>
show adoption log [adoptee|adopter {<MAC>}] {on <DEVICE-NAME>}
show adoption [controllers|history|info|pending|status|timeline] {on
<DEVICE-NAME>}
```

Parameters

`show adoption offline`

adoption	Displays adoption related information. It also displays configuration errors.
offline	Displays non-adopted status of the logged device and its adopted access points

`show adoption config-errors <DEVICE-NAME>`

adoption	Displays adoption related information. It also displays configuration errors.
config-errors <DEVICE-NAME>	Displays configuration errors for a specified adopted device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`show adoption log [adoptee|adopter] {on <DEVICE-NAME>}`

adoption	Displays adoption related information. It also displays configuration errors.
log [adoptee|adopter] {on <DEVICE-NAME>}	Displays adoption logs, for the specified device. If no device name is specified, the system displays logs for the logged device. • adoptee – Displays adoption logs for adoptee devices (APs, wireless controllers, and service platforms). To view logs for a specified adoptee, specify the device's name. If no device name is specified, the system displays logs for the logged device. If the logged device is not an adoptee, the system states that the device is a controller. For example, `2013-01-19 22:00:13:MLCP_TAG_CLUSTER_MASTER not present and this device is a controller. Ignoring` • on <DEVICE-NAME> – Optional. Displays adoptee status and details for the device identified by the <DEVICE-NAME> keyword • adopter – Displays adoption logs for adopter devices (APs, wireless controllers, and service platforms). To view logs for a specified adopter, specify the device's name. If no device name is specified, the system displays logs for the logged device. • <MAC> – Optional. Filters adopters by the adoptee device's MAC address. Specify the adoptee device's MAC address. The system displays logs for the device that has adopted the device identified by the <MAC> keyword. • on <DEVICE-NAME> – Optional. Displays adopter status and details for the device identified by the <DEVICE-NAME> keyword. Specify the adopter device's name. A wireless controller or service platform cannot be configured as an adoptee and an adopter simultaneously. In other words, an adopted wireless controller or service platform cannot be configured to adopt another device and vice versa.

`show adoption [history|controllers|info|pending|status|timeline] {on <DEVICE-NAME>}`

adoption	Displays adoption related information. It also displays configuration errors.
controllers	Displays information about adopted controllers. This is applicable in a Hierarchically managed network, where site controllers are adopted by the NOC controllers.
history	Displays adoption history of the logged device and its adopted access points
info	Displays adopted device information
pending	Displays information for devices pending adoption
status	Displays adoption status for logged devices
timeline	Displays the logged device's adoption timeline. It also shows the adoption time for logged device's adopted APs. To view the adoption timeline of a specific device, use the *on <device-name>* option to specify the device.
on <DEVICE-NAME>	The following keywords are common to all of the above parameters: • on <DEVICE-NAME> – Optional. Displays a device's adoption information, based on the parameter passed. • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Example

```
rfs4000-229D58(config)#show adoption offline
-------------------------------------------------------------------------------
------------------
        MAC           HOST-NAME        TYPE       RF-DOMAIN            TIME
OFFLINE
-------------------------------------------------------------------------------
------------------
-------------------------------------------------------------------------------
------------------
Total number of devices displayed: 2
rfs4000-229D58(config)#

rfs4000-229D58(config)#show adoption log adoptee on rfs4000-229D58
2013-03-15 12:47:07:DNS resolution completed, starting MLCP
2013-03-15 12:47:07:Received 0 hostnames through option 192
2013-03-15 12:47:07:Changing adoption state from Disabled to No adopters found
2013-03-15 12:47:07:DNS resolution completed, starting MLCP
2013-03-15 12:47:07:Adoption enabled due to configuration
rfs4000-229D58(config)#

rfs7000-19C875>show adoption controllers
-------------------------------------------------------------------------------
---------------------------------
             NAME     RF-DOMAIN               MAC      MINT-ID
IP           ADOPTED-BY
-------------------------------------------------------------------------------
---------------------------------
     rfs4000-229BA0          rfs4k   00-23-68-22-9B-A0   68.22.9B.A0
192.168.200.70       rfs7000-37FA7D
      nx6524-4A8814            bob   B4-C7-99-4A-88-14   19.4A.88.14
192.168.200.72       rfs7000-19C875
     rfs4000-6FA2D4          rfs4k   B4-C7-99-6F-A2-D4   19.6F.A2.D4
192.168.200.71       rfs7000-19C875
-------------------------------------------------------------------------------
---------------------------------
Total number of devices displayed: 3

rfs7000-19C875>
```

advanced-wips

show commands

Displays advanced *Wireless Intrusion Prevention Policy* (WIPS) settings

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — , Brocade Mobility RFS9510

Syntax:

```
show advanced-wips [configuration|stats]
```

```
show advanced-wips configuration [events {thresholds}|terminate-list]

show advanced-wips stats
[br-table|client-table|connected-sensors|detected-aps|
          detected-clients-for-br|event-history|server-listening-port]
show advanced-wips stats
[br-table|client-table|connected-sensors|event-history|
          server-listening-port]
show advanced-wips stats [detected-aps|detected-clients-for-br <BSS-ID>]
          {neighboring|sanstioned|unsanctioned}
```

Parameters

`show advanced-wips configuration [events {thresholds}|terminate-list]`

configuration	Displays advanced WIPS settings
events thresholds	Displays events summary Advanced WIPS policies assigned to controllers support various events depending on the configuration. These events are individually triggered against authorized, unauthorized, and neighboring devices. • thresholds – Optional. Displays threshold values for each event configured in the advanced WIPS policy
terminate-list	Displays the terminate list

`show advanced-wips stats [br-table|client-table|connected-sensors|event-history| server-listening-port]`

stats	Displays advanced WIPS statistics
br-table	Displays AP table statistics
client-table	Displays station table statistics
connected-sensors	Displays connected sensors statistics
event-history	Displays advanced WIPS event history
server-listening-port	Displays advanced WIPS server listening port statistics

`show advanced-wips stats [detected-aps|detected-clients-for-br <BSS-ID>] {neighboring|sanstioned|unsanctioned}`

stats	Displays advanced WIPS statistics
detected-aps	Displays detected AP details, based on the parameters passed • neighboring – Optional. Displays neighboring AP statistics • sanctioned – Optional. Displays sanctioned AP statistics • unsanctioned – Optional. Displays unsanctioned AP statistics
detected-clients-for-br <BSS-ID>	Displays clients statistics for APs, based on the parameters passed • <BSS-ID> – Displays clients for a specified AP. Enter the AP's BSS ID in the AA-BB-CC-DD-EE-FF format. • neighboring – Optional. Displays neighboring client information • sanctioned – Optional. Displays sanctioned client information • unsanctioned – Optional. Displays unsanctioned client information

Example

```
rfs7000-37FABE(config)#show advanced-wips configuration events
------------------------------------------------------------------------------
-----------------------
```

```
 POLICY SLNO                      NAME                      TRIGGER-S TRIGGER-U
TRIGGER-N MITIGATION
--------------------------------------------------------------------------------
-----------------------
  test   1   essid-jack-attack-detected               N       N       N
-
  test   2   unauthorized-bridge                     N       N       N
-
  test   3   wlan-jack-attack-detected               N       N       N
-
  test   4   multicast-igrp-routers-detection         N       N       N
-
  test   5   multicast-igmp-detection                N       N       N
-
  test   6   dos-eapol-logoff-storm                  N       N       N
-
  test   7   probe-response-flood                    N       N       N
-
  test   8   monkey-jack-attack-detected             N       N       N
-
  test   9    dos-rts-flood                               N         N
--More--
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show advanced-wips configuration events thresholds
--------------------------------------------------------------------------------
---
  POLICY    #             EVENT                    THRESHOLD            VALUE
--------------------------------------------------------------------------------
---
  test     1     dos-eapol-logoff-storm     eapol-start-frames-br      10
  test     2     dos-eapol-logoff-storm     eapol-start-frames-mu      5
  test     3     probe-response-flood       probe-rsp-frames-count     50
  test     4     dos-cts-flood              cts-frames-ratio           70
  test     5     dos-cts-flood              mu-rx-cts-frames           20
  -        -     -                          -                          -
--------------------------------------------------------------------------------
---
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show advanced-wips stats detected-aps
Number of APs: 0
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show advanced-wips stats client-table
Number of clients: 2
rfs7000-37FABE(config)#
```

boot

show commands

Displays a device's boot configuration. Use this command to view the primary and secondary image details, such as Build Date, Install Date, and Version. This command also displays the current boot and next boot information.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show boot {on <DEVICE-NAME>}
```

Parameters

```
show boot {on <DEVICE-NAME>}
```

boot	Displays primary and secondary image boot configuration details (build date, install date, version, and the image used to boot the current session)
on <DEVICE-NAME>	Optional. Displays a specified device's boot configuration • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. **NOTE:** Use the *on <DEVICE-NAME>* option to view a remote device's boot configuration.

Example

```
rfs4000-229D58(config)#show boot
------------------------------------------------------------------------------
---
     IMAGE            BUILD DATE             INSTALL DATE          VERSION
------------------------------------------------------------------------------
---
  Primary       04:09:2013 12:40:41     04:10:2013 09:10:05     5.5.0.0-034B
  Secondary     03:31:2013 02:46:47     04:04:2013 10:45:00     5.5.0.0-030D
------------------------------------------------------------------------------
---
Current Boot       : Primary
Next Boot          : Primary
Software Fallback  : Enabled
rfs4000-229D58(config)#
```

captive-portal

show commands

Displays WLAN captive portal information. Use this command to view a configured captive portal's client information.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show captive-portal client {filter|on|satistics}

show captive-portal client {filter} {captive-portal|ip|state|vlan|wlan}

show captive-portal client {filter} {captive-portal [<CAPTIVE-PORTAL>|
          not <CAPTIVE-PORTAL>]}

show captive-portal client {filter} {ip [<IP>|not <IP>]}

show captive-portal client {filter} {state
[pending|success|not[pending|success]]}

show captive-portal client {filter} {vlan [<VLAN-ID>|not <VLAN-ID>]}

show captive-portal client {filter} {wlan [<WLAN-NAME>|not <WLAN-NAME>]}

show captive-portal client {on <DEVICE-OR-DOMAIN-NAME>|statistics} {filter}
          {captive-portal|ip|state|vlan|wlan}
```

Parameters

`show captive-portal client {filter} {captive-portal [<CAPTIVE-PORTAL>| not <CAPTIVE-PORTAL>]}`

captive-portal client	Displays captive portal client information
filter	Optional. Defines additional filters
captive-portal [<CAPTIVE-PORTAL>| not <CAPTIVE-PORTAL>]	Optional. Displays captive portal client information, based on the captive portal name passed • <CAPTIVE-PORTAL> – Displays client details for a captive portal specified by the <CAPTIVE-PORTAL> parameter • not <CAPTIVE-PORTAL> – Inverts the match selection

`show captive-portal client {filter} {ip [<IP>|not <IP>]}`

captive-portal client	Displays captive portal client information
filter	Optional. Defines additional filters
ip [<IP>|not <IP>]	Optional. Displays captive portal client information, based on the IP address passed • <IP> – Specify the client's IP address • not <IP> – Inverts the match selection

`show captive-portal client {filter} {state [pending|success|not [pending|success]]}`

captive-portal client	Displays captive portal client information
filter	Optional. Defines additional filters
state	Optional. Filters clients based on their state of authentication
pending	Displays clients redirected for authentication
success	Displays successfully authenticated clients
not [pending|success]]	Inverts match selection • pending – Displays successfully authenticated clients (opposite of pending authentication) • success – Displays clients redirected for authentication (opposite of successful authentication)

`show captive-portal client {filter} {vlan [<VLAN-ID>|not <VLAN-ID>]}`

captive-portal client	Displays captive portal client information
filter	Optional. Defines additional filters
vlan [<VLAN-ID>| not <VLAN-ID>]	Optional. Displays captive portal clients based on the VLAN ID passed • <VLAN-ID> – Specify the VLAN ID. • not <VLAN-ID> – Inverts match selection

`show captive-portal client {filter} {wlan [<WLAN-NAME>|not <WLAN-NAME>]}`

captive-portal client	Displays captive portal client information
filter	Optional. Defines additional filters
wlan [<WLAN-NAME>| not <WLAN-NAME>]	Optional. Displays captive portal clients based on the WLAN name passed • <WLAN-NAME> – Specify the WLAN name. • not <WLAN-NAME> – Inverts match selection

`show captive-portal client {on <DEVICE-OR-DOMAIN-NAME>|statistics} {filter} {captive-portal|ip|state|vlan|wlan}`

captive-portal client	Displays captive portal client information
on <DEVICE-OR-DOMAIN-NAME>	Optional. Displays captive portal clients on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.
statistics	Optional. Displays captive portal client statistics. This feature enables monitoring of a captive portal client's data usage. When enabled, it provides a client's data transmission (both upstream and downstream) details, without considering the dot11 overhead for each packet.
filter	The following keywords are common to the 'on' and 'statistics' parameters: • filter – Optional. Defines additional filters • captive-portal – Optional. Displays captive portal client information for a specified captive portal • ip – Optional. Displays captive portal client information based on IP address passed • state – Optional. Displays captive portal client information based on the their authentication state • vlan – Displays captive portal clients on a specified VLAN • wlan – Optional. Displays captive portal clients on a specified WLAN

Example

```
rfs4000-229D58#show captive-portal client on rfs4000-229D58
================================================================================
RF-Domain: test
CLIENT                  IP     CAPTIVE-PORTAL     WLAN             VLAN
STATE SESSION TIME
--------------------------------------------------------------------------------
----------------------------------
44-6D-57-08-25-4A    10.10.10.183 test             wlan-br7131-cp    1
Pending      0:00:00
--------------------------------------------------------------------------------
----------------------------------
RF-Domain: test, sub-total of captive portal clients displayed = 1
================================================================================

================================================================================
RF-Domain: default
CLIENT                  IP     CAPTIVE-PORTAL     WLAN             VLAN
STATE SESSION TIME
--------------------------------------------------------------------------------
----------------------------------
```

```
--------------------------------------------------------------------------------
----------------------------------
RF-Domain: default, sub-total of captive portal clients displayed = 0
================================================================================

================================================================================
RF-Domain: new-l3-rf-dmn
CLIENT                  IP     CAPTIVE-PORTAL     WLAN             VLAN
STATE SESSION TIME
--------------------------------------------------------------------------------
----------------------------------
00-24-D7-EC-CF-78    10.10.10.175 CP1              rfs-with-radio    1
Success     22:50:38
--------------------------------------------------------------------------------
----------------------------------
RF-Domain: new-l3-rf-dmn, sub-total of captive portal clients displayed = 1
================================================================================

Total number of captive portal clients displayed: 2

rfs4000-229D58#

rfs4000-229D58#show captive-portal client statistics
================================================================================
RF-Domain: test
CLIENT                  IP     CAPTIVE-PORTAL         TX-PKTS     TX-BYTES
RX-PKTS     RX-BYTES
--------------------------------------------------------------------------------
----------------------------------
44-6D-57-08-25-4A    10.10.10.183 test                    0          0
0            0
--------------------------------------------------------------------------------
----------------------------------
RF-Domain: test, sub-total of captive portal clients displayed = 1
================================================================================

================================================================================
RF-Domain: default
CLIENT                  IP     CAPTIVE-PORTAL         TX-PKTS     TX-BYTES
RX-PKTS     RX-BYTES
--------------------------------------------------------------------------------
----------------------------------
--------------------------------------------------------------------------------
----------------------------------
RF-Domain: default, sub-total of captive portal clients displayed = 0
================================================================================

================================================================================
RF-Domain: new-l3-rf-dmn
CLIENT                  IP     CAPTIVE-PORTAL         TX-PKTS     TX-BYTES
RX-PKTS     RX-BYTES
--------------------------------------------------------------------------------
----------------------------------
00-24-D7-EC-CF-78    10.10.10.175 CP1                     119       11419
26554      1396167
--------------------------------------------------------------------------------
----------------------------------
RF-Domain: new-l3-rf-dmn, sub-total of captive portal clients displayed = 1
================================================================================
```

```
Total number of captive portal clients displayed: 2
rfs4000-229D58#
```

captive-portal-page-upload

show commands

Displays captive portal page information, such as upload history, upload status, and page file download status

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show captive-portal-page-upload [history|load-image-status|status]
show captive-portal-page-upload load-image-status
show captive-portal-page-upload history {on <RF-DOMAIN-NAME>}
show captive-portal-page-upload status {on
[<RF-DOMAIN-NAME>|<RF-DOMAIN-MANAGER>]}
```

Parameters

```
show captive-portal-page-upload load-image-status
```

load-image-status	Displays captive portal advanced page file download status on the logged device

```
show captive-portal-page-upload history {on <RF-DOMAIN-NAME>}
```

history {on <RF-DOMAIN-NAME>}	Displays captive portal page upload history • on <RF-DOMAIN-NAME> – Optional. Displays captive portal page upload history within a specified RF Domain. Specify the RF Domain name.

```
show captive-portal-page-upload status {on
[<RF-DOMAIN-NAME>|<RF-DOMAIN-MANAGER>]}
```

status {on <RF-DOMAIN-NAME>| on <RF-DOMAIN-MANAGER>}	Displays captive portal page upload status • on <RF-DOMAIN-NAME> – Optional. Displays captive portal page upload status within a specified RF Domain. Specify the RF Domain name. • on <RF-DOMAIN-MANAGER> – Optional. Displays captive portal page upload status for a specified RF Domain Manager. Specify the RF Domain Manager name.

Example

```
rfs7000-37FABE>show captive-portal-page-upload status
Number of APs currently being uploaded : 0
Number of APs waiting in queue to be uploaded : 0
--------------------------------------------------------------------------------
---
  AP STATE  UPLOAD TIME   PROGRESS RETRIES  LAST UPLOAD ERROR    UPLOADED BY
--------------------------------------------------------------------------------
---
```

```
-------------------------------------------------------------------------------
---
rfs7000-37FABE>

rfs7000-37FABE>show captive-portal-page-upload history
-------------------------------------------------------------------------------
----------
     AP      RESULT                 TIME  RETRIES        UPLOADED-BY
LAST-UPLOAD-ERROR
-------------------------------------------------------------------------------
----------
No upload history is present
rfs7000-37FABE>

rfs7000-37FABE>show captive-portal-page-upload load-image-status
No captive portal advanced page file download is in progress
rfs7000-37FABE>
```

cdp

show commands

Displays the *Cisco Discovery Protocol* (CDP) neighbor table

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show cdp [neighbors|report] {detail {on <DEVICE-NAME>}|on <DEVICE-NAME>}
```

Parameters

```
show cdp [neighbors|report] {detail {on <DEVICE-NAME>}|on <DEVICE-NAME>}
```

cdp [neighbors|report]	Displays CDP neighbors table or aggregated CDP neighbors table
detail {on <DEVICE-NAME>}	Optional. Displays detailed CDP neighbors table or aggregated CDP neighbors table • on <DEVICE-NAME> – Optional. Displays table details on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.
on <DEVICE-NAME>	Optional. Displays table details on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Example

```
The following example shows detailed CDP neighbors table:

rfs7000-37FABE(config)#show cdp neighbors detail on rfs7000-37FABE
-------------------------
Device ID: br7131-11E6C4
Entry address(es):
  IP Address: 172.16.10.23
  IP Address: 172.16.20.1
```

```
  IP Address: 169.254.230.196
Platform: Brocade Mobility 7131 Access Point, Capabilities: Router Switch
Interface: ge1, Port ID (outgoing port): ge1
Hold Time: 131 sec

advertisement version: 2
Native VLAN: 1
Duplex: full
Version :
5.4.1.0-018R
-------------------------
Device ID: br7131-139B34
Entry address(es):
  IP Address: 172.16.10.22
Platform: AP7131N, Capabilities: Router Switch
Interface: ge1, Port ID (outgoing port): ge1
Hold Time: 129 sec

--More--
rfs7000-37FABE(config)#

The following example shows a non-detailed CDP neighbors table:

rfs7000-37FABE(config)#show cdp neighbors on rfs7000-37FABE
------------------------------------------------------------------------------
---
    Device ID     Neighbor IP    Platform   Local Intrfce   Port ID    Duplex
------------------------------------------------------------------------------
---
 br7131-11E6C4   172.16.10.23   AP7131     ge1             ge1        full
 br7131-139B34   172.16.10.22   AP7131N    ge1             ge1        full
------------------------------------------------------------------------------
---
rfs7000-37FABE(config)#
```

clock

show commands

Displays a selected system's clock

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show clock {on <DEVICE-NAME>}
```

Parameters

```
show clock {on <DEVICE-NAME>}
```

clock	Displays a system's clock
on <DEVICE-NAME>	Optional. Displays system clock on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

Example

```
rfs7000-37FABE(config)#show clock
2013-02-15 15:38:47 UTC
rfs7000-37FABE(config)#
```

cluster

show commands

Displays cluster information (cluster configuration parameters, members, status etc.)

Supported in the following platforms:

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show cluster [configuration|members|status]
show cluster [configuration|members {detail}|status]
```

Parameters

```
show cluster [configuration|members {detail}|status]
```

cluster	Displays cluster information
configuration	Displays cluster configuration parameters
members {detail}	Displays cluster members configured on the logged device • detail – Optional. Displays detailed information of known cluster members
status	Displays cluster status

Example

```
rfs7000-37FABE(config)#show cluster configuration

Cluster Configuration Information
 Name                          : Cluster1
 Configured Mode               : Active
 Master Priority               : 128
 Force configured state        : Disabled
 Force configured state delay  : 5 minutes
 Handle STP                    : Disabled
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show cluster members detail
------------------------------------------------------------------------------
---
      ID     MAC    MODE   AP COUNT AAP COUNT AP LICENSE AAP LICENSE
VERSION
```

```
-------------------------------------------------------------------------------
---                              -------------------------
 70.37.FA.BE  00-15-70-37-FA-BE  Active  0    0     50     50
5.4.2.0-006D

-------------------------------------------------------------------------------
---                              -------------------------
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show cluster status

Cluster Runtime Information
 Protocol version             : 1
 Cluster operational state    : active
 AP license                   : 0
 AAP license                  : 0
 AP count                     : 0
 AAP count                    : 0
 Max AP adoption capacity     : 1024
 Number of connected member(s): 0
rfs7000-37FABE(config)#
```

commands

show commands

Displays commands available for the current mode

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show commands
```

Parameters

None

Example

```
rfs4000-229D58(config)#show commands
  help
  help search WORD (|detailed|only-show|skip-show|skip-no)
  show commands
  show adoption log adoptee(|(on DEVICE-NAME))
  show adoption log adopter (|mac AA-BB-CC-DD-EE-FF)(|(on DEVICE-NAME))
  show adoption info (|(on DEVICE-NAME))
  show adoption status (|(on DEVICE-NAME))
  show adoption config-errors DEVICE-NAME
  show adoption offline
  show adoption pending (|(on DEVICE-NAME))
  show adoption history (|(on DEVICE-NAME))
```

```
  show debugging (|(on DEVICE-OR-DOMAIN-NAME))
  show debugging cfgd
  show debugging fib(|(on DEVICE-NAME))
  show debugging adoption (|(on DEVICE-OR-DOMAIN-NAME))
  show debugging wireless (|(on DEVICE-OR-DOMAIN-NAME))
  show debugging snmp (|(on DEVICE-NAME))
  show debugging ssm (|(on DEVICE-NAME))
  show debugging voice (|(on DEVICE-OR-DOMAIN-NAME))
  show debugging captive-portal (|(on DEVICE-OR-DOMAIN-NAME))
  show debugging dhcpsvr (|(on DEVICE-NAME))
  show debugging role (|(on DEVICE-OR-DOMAIN-NAME))
  show debugging dot1x(|(on DEVICE-NAME))
--More--
rfs4000-229D58(config)#

nx4500-5CFA2B(config)#show commands
  help
  help search WORD (|detailed|only-show|skip-show|skip-no)
  show commands
  show adoption log adoptee(|(on DEVICE-NAME))
  show adoption log adopter (|mac AA-BB-CC-DD-EE-FF)(|(on DEVICE-NAME))
  show adoption info (|(on DEVICE-NAME))
  show adoption status (|(on DEVICE-NAME))
  show adoption config-errors DEVICE-NAME
  show adoption offline
  show adoption pending (|(on DEVICE-NAME))
  show adoption history (|(on DEVICE-NAME))
  show debugging (|(on DEVICE-OR-DOMAIN-NAME))
  show debugging cfgd
  show debugging fib(|(on DEVICE-NAME))
  show debugging adoption (|(on DEVICE-OR-DOMAIN-NAME))
  show debugging wireless (|(on DEVICE-OR-DOMAIN-NAME))
--More--
nx4500-5CFA2B(config)#
```

context

show commands

Displays the current context details

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show context {include-factory|session-config {include-factory}}
```

Parameters

	show context *{include-factory|session-config {include-factory}}*
include-factory	Optional. Includes factory defaults
session-config include-factory	Optional. Displays running system information in the current context • include-factory – Optional. Includes factory defaults

Example

```
rfs4000-229D58(config)#show context
!
! Configuration of Brocade Mobility RFS4000 version 5.5.0.0-034B
!
!
version 2.3
!
!
client-identity TestClientIdentity
 dhcp 1 message-type request option-codes exact hexstring 5e4d36780b3a7f
!
client-identity-group ClientIdentityGroup
 client-identity TestClientIdentity precedence 1
!
alias network testNetworklAlias address-range 192.168.13.4 to 192.168.13.10
!
ip access-list BROADCAST-MULTICAST-CONTROL
 permit tcp any any rule-precedence 10 rule-description "permit all TCP
traffic"
 permit udp any eq 67 any eq dhcpc rule-precedence 11 rule-description "permit
DHCP replies"
 deny udp any range 137 138 any range 137 138 rule-precedence 20
rule-description "deny windows netbios"
 deny ip any 224.0.0.0/4 rule-precedence 21 rule-description "deny IP
multicast"
 deny ip any host 255.255.255.255 rule-precedence 22 rule-description "deny IP
l
--More--
rfs4000-229D58(config)#
```

critical-resources

show commands

Displays critical resource information. Critical resources are resources vital to the network.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show critical-resources {on <DEVICE-NAME>}
```

Parameters

```
show critical-resources {on <DEVICE-NAME>}
```

critical-resources	Displays critical resources information
on <DEVICE-NAME>	Optional. Displays critical resource information on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Example

```
rfs4000-229D58(config)#show critical-resources on rfs4000-229D58
--------------------------------------------------------------------------------
CRITICAL RESOURCE IP        VLAN          PING-MODE            STATE
--------------------------------------------------------------------------------
172.168.1.103                1             arp-icmp             up
--------------------------------------------------------------------------------
rfs4000-229D58(config)#
```

crypto

show commands

Displays encryption mode information

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show crypto [ike|ipsec|key|pki]

show crypto ike sa {detail|on|peer|version}
show crypto ike sa {detail|peer <IP>} {on <DEVICE-NAME>}
show crypto ike sa {version [1|2]} {peer <IP>} {(on <DEVICE-NAME>)}

show crypto ipsec sa {detail|on|peer}
show crypto ipsec sa {detail} {on <DEVICE-NAME>}
show crypto ipsec sa {peer <IP>} {detail} {(on <DEVICE-NAME>)}

show crypto key rsa {on|public-key-detail}
show crypto key rsa {public-key-detail} {(on <DEVICE-NAME>)}

show crypto pki trustpoints {<TRUSTPOINT-NAME>|all|on}
show crypto pki trustpoints {<TRUSTPOINT-NAME>|all} {(on <DEVICE-NAME>)}
```

Parameters

```
show crypto ike sa {detail|peer <IP>} {on <DEVICE-NAME>}
```

crypto ike sa	Displays *Internet Key Exchange* (IKE) *security association* (SA) statistics
detail	Displays detailed IKE SA statistics

peer <IP>	Optional. Displays IKE SA statistics for a specified peer • <IP> – Specify the peer's IP address in the A.B.C.D format
on <DEVICE-NAME>	Optional. Displays IKE SA statistics on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`show crypto ike sa {version [1|2]} {peer <IP>} {(on <DEVICE-NAME>)}`

crypto ike sa	Displays IKE SA details
version [1|2]	Optional. Displays IKE SA version statistics • 1 – Displays IKEv1 statistics • 2 – Displays IKEv2 statistics
peer <IP>	Optional. Displays IKE SA version statistics for a specified peer • <IP> – Specify the peer's IP address in the A.B.C.D format
on <DEVICE-NAME>	The following keyword is recursive and common to the 'peer ip' parameter: • on <DEVICE-NAME> – Optional. Displays IKE SA statistics on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`show crypto ipsec sa {detail} {on <DEVICE-NAME>}`

crypto ipsec sa	Displays *Internet Protocol Security* (IPSec) SA statistics. The IPSec encryption authenticates and encrypts each IP packet in a communication session
detail	Optional. Displays detailed IPSec SA statistics
on <DEVICE-NAME>	Optional. Displays IPSec SAs on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`show crypto sa {peer <IP>} {detail} {(on <DEVICE-NAME>)}`

crypto ipsec sa	Displays IPSec SA statistics. The IPSec encryption authenticates and encrypts each IP packet in a communication session
peer <IP> detail	Optional. Displays IPSec SA statistics for a specified peer • <IP> – Specify the peer's IP address in the A.B.C.D format. • detail – Displays detailed IPSec SA statistics for the specified peer
on <DEVICE-NAME>	The following keyword is recursive: • on <DEVICE-NAME> – Optional. Displays IPSec SAs on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`show crypto key rsa {public-key-detail} {(on <DEVICE-NAME>)}`

crypto key rsa	Displays RSA public keys
public-key-detail	Optional. Displays public key in the *Privacy-Enhanced Mail* (PEM) format
on <DEVICE-NAME>	The following keyword is recursive: • on <DEVICE-NAME> – Optional. Displays public key on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`show crypto pki trustpoints {<TRUSTPOINT-NAME>|all} {(on <DEVICE-NAME>)}`

crypto pki	Displays PKI related information
trustpoints	Displays WLAN trustpoints
<TRUSTPOINT-NAME>	Optional. Displays a specified trustpoint details. Specify the trustpoint name.

all	Optional. Displays details of all trustpoints
on <DEVICE-NAME>	The following keyword is recursive and common to the 'trustpoint-name' and 'all' parameters: • on <DEVICE-NAME> – Optional. Displays trustpoints configured on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Example

```
rfs7000-37FABE(config)#show crypto key rsa public-key-detail on rfs7000-37FABE

RSA key name: test1        Key-length: 1032
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQL+qxgk4HLK7XRKokIinDCiRIaZ
rE1aUGMI9iQJGSQakhV3WxP1V8NsrAn1uhojPMoBYTddAqOTgNnQxvrMOnd7yV+3
lXQomy3Xb0wLj0KSp6CPOZgXHbWrUSNP3K7fNAKSYjQ0LlAJTcvitKRe0yfLCsJd
9HZF4Hxum1ktOFy93wIDAQAB
-----END PUBLIC KEY-----


RSA key name: mint_security_trustpoint-srvr-priv-key        Key-length: 1024
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/zlGeiIM0YagLvkviEQFnd/lf
6aw1S+xQN1DugLJQgA27ylnCJtM5YeUKQD+lmjCvXr9Ku+bAxLnVWF3FpvttZgsH
J3dOytzedJ/VuRJYCO2ChWYoUdtTSfuyK/srzkSU2akiOyp9jCXUeL/A8w1RRUBE
cNeRYDtQPEocHImmhwIDAQAB
-----END PUBLIC KEY-----


RSA key name: default-trustpoint-srvr-priv-key        Key-length: 1024
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDGHBR2bxLeRZ4G6hm7jHJRSaeE
A216r4s4qptiSld+rKeMihPTFbYELedk3dITkzF1EU7Ov0vKzant0pyAmdJ8ci//
--More--

rfs7000-37FABE(config)#show crypto key rsa on rfs7000-37FABE
+------------+-------------------------------------------+----------------
|     #      |                 KEY NAME                  |      KEY LENGTH     |
+------------+-------------------------------------------+----------------
| 1          | default-trustpoint-srvr-priv-key          | 1024               |
| 2          | default_rsa_key                           | 1024               |
+------------+-------------------------------------------+------------------
--+
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show crypto pki trustpoints all on rfs7000-37FABE

Trustpoint Name: mint_security_trustpoint        (on-board CA)
-------------------------------------------------------------------------------
--
  CRL present: no
  Server Certificate details:
    Key used: mint_security_trustpoint-srvr-priv-key
    Serial Number: 7037fabe03
    Subject Name:
      CN=70.37.fa.be, C=US, O=Brocade
    Issuer Name:
      CN=70.37.fa.be:2010-04-26-15-00-39, C=US, O=Brocade
    Valid From : Mon Apr 26 15:00:41 2010 UTC
    Valid Until: Tue Apr 26 15:00:41 2011 UTC
```

```
  CA Certificate details:
    Serial Number: 01
    Subject Name:
      CN=70.37.fa.be:2010-04-26-15-00-39, C=US, O=Brocade
    Issuer Name:
      CN=70.37.fa.be:2010-04-26-15-00-39, C=US, O=Brocade
    Valid From : Mon Apr 26 15:00:39 2010 UTC
    Valid Until: Tue Apr 26 15:00:39 2011 UTC
--More--
rfs7000-37FABE(config)#
```

device-upgrade

show commands

Displays device firmware upgradation information for devices adopted by a wireless controller or access point

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show device-upgrade [history|load-image-status|status|versions]
```

Parameters

```
show device-upgrade [history|load-image-status|status|versions]
```

device-upgrade	Displays device upgrade information based on the parameters passed
history	Displays device upgrade history

load-image-status	Displays firmware image loading status. The output displays the <DEVICE> image loading status in percentage.
	For example:
	`#show device-upgrade load-image-status`
	`Download of br81xx firmware file is 47 percent complete`

status	Displays device firmware upgrade status
versions	Displays firmware image versions

Example

```
rfs4000-229D58#show device-upgrade versions
------------------------------------------------------------------------------
---
           CONTROLLER               DEVICE-TYPE               VERSION
------------------------------------------------------------------------------
---
  00-23-68-22-9D-58            rfs4000              none
00-23-68-22-9D-58            br1220               5.5.0.0-018D
00-23-68-22-9D-58            rfs6000              none
```

```
00-23-68-22-9D-58            br71xx               none
  00-23-68-22-9D-58            br6511               none
  00-23-68-22-9D-58            rfs7000              none
  00-23-68-22-9D-58            br650                5.5.0.0-018D
  00-23-68-22-9D-58            br81xx               none
-------------------------------------------------------------------------------
---
rfs4000-229D58#

rfs4000-229D58#show device-upgrade history
-------------------------------------------------------------------------------
--------------------
           Device      RESULT               TIME  RETRIES       UPGRADED-BY
LAST-UPDATE-ERROR
-------------------------------------------------------------------------------
--------------------

     ap6532-986C50      failed  2012-01-05 00:26:31       3     rfs4000-229D58
Update error:  Bad file, failure in tar. tar: invalid tar magic

     br71xx-0F43D8      failed  2012-01-05 00:21:08       3     rfs4000-229D58
Update error:  Unable to get update file, failure in ftp/openssl/tar
Total number of entries displayed: 2
rfs4000-229D58#

rfs4000-229D58#show device-upgrade status
'Number of devices currently being upgraded : 0
Number of devices waiting in queue to be upgraded : 0
Number of devices currently being rebooted : 0
Number of devices waiting in queue to be rebooted : 0
-------------------------------------------------------------------------------
-------------
 DEVICE STATE UPGRADE TIME REBOOT TIME PROGRESS RETRIES LAST UPDATE ERROR
UPGRADED BY
-------------------------------------------------------------------------------
-------------
-------------------------------------------------------------------------------
-------------
rfs4000-229D58#

nx4500-5CFA2B(config)#show device-upgrade versions
-------------------------------------------------------------------------------
---
          CONTROLLER               DEVICE-TYPE                VERSION
-------------------------------------------------------------------------------
---
nx4500-5CFA2B              br650                  5.5.0.0-034B
nx4500-5CFA2B              br6511                 5.5.0.0-034B
nx4500-5CFA2B              br1220                 5.5.0.0-034B
nx4500-5CFA2B              br71xx                 5.5.0.0-034B
nx4500-5CFA2B              br81xx                 5.5.0.0-034B
-------------------------------------------------------------------------------
---
nx4500-5CFA2B(config)#
```

dot1x

show commands

Displays dot1x information on interfaces

Dot1x (or 802.1x) is an IEEE standard for network authentication. Devices supporting dot1x allow the automatic provision and connection to the wireless network without launching a Web browser at login. When within range of a dot1x network, a device automatically connects and authenticates without needing to manually login.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

NOTE
Dot.1x supplicant configuration is supported on the following platforms:
- Access Points – Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers – Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

NOTE
Dot.1x authenticator configuration is supported on the following platforms:
- Access Points – Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers – Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

```
show dot1x {all|interface|on}

show dot1x {all {on <DEVICE-NAME>}|on <DEVICE-NAME>}
show dot1x {interface [<INTERFACE-NAME>|ge <1-4>|port-channel <1-2>}
           {on <DEVICE-NAME>}
```

Parameters

```
show dot1x {all {on <DEVICE-NAME>}|on <DEVICE-NAME>}
```

dot1x all {on <DEVICE-NAME>}	Optional. Displays dot1x information for all interfaces • on <DEVICE-NAME> – Optional. Displays dot1x information for all interfaces on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.
dot1x {on <DEVICE-NAME>}	Optional. Displays dot1x information for interfaces on a specified device • <DEVICE-NAME> – Specify the name of AP, wireless controller, or service platform.

```
show dot1x {interface [<INTERFACE-NAME>|ge <1-4>|port-channel <1-2>]} {on
<DEVICE-NAME>}
```

dot1x interface	Optional. Displays dot1x information for a specified interface or interface type
<INTERFACE-NAME>	Displays dot1x information for the layer 2 (Ethernet port) interface specified by the <INTERFACE-NAME> parameter
ge <1-4>	Displays dot1x for a specified GigabitEthernet interface • <1-4> – Select the interface index from 1 - 4.

port-channel <1-2>	Displays dot1x for a specified port channel interface • <1-2> – Select the interface index from 1 - 2.
on <DEVICE-NAME>	The following keywords are common to all of the above parameters: • on <DEVICE-NAME> – Optional. Displays dot1x interface information on a specified device • <DEVICE-NAME> – Specify the name of AP, wireless controller, or service platform.

Example

```
rfs7000-37FABE(config)#show dot1x all on rfs7000-37FABE
SysAuthControl is disabled
Guest-Vlan is disabled
AAA-Policy is none

Dot1x info for interface GE1
-----------------------------------
Supplicant MAC N/A
  Auth SM State = FORCE AUTHORIZED
  Bend SM State = REQUEST
  Port Status   = AUTHORIZED
  Host Mode     = SINGLE
  Auth Vlan     = None
  Guest Vlan    = None

Dot1x info for interface GE2
-----------------------------------
Supplicant MAC N/A
  Auth SM State = FORCE AUTHORIZED
  Bend SM State = REQUEST
  Port Status   = AUTHORIZED
  Host Mode     = SINGLE
  Auth Vlan     = None
  Guest Vlan    = None
--More--
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show dot1x interface ge 3
Dot1x info for interface GE3
-----------------------------------
Supplicant MAC N/A
  Auth SM State = FORCE AUTHORIZED
  Bend SM State = REQUEST
  Port Status   = AUTHORIZED
  Host Mode     = SINGLE
  Auth Vlan     = None
  Guest Vlan    = None

rfs7000-37FABE(config)#
```

environmental-sensor

show commands

Displays environmental sensor's recorded data. The environmental sensor has to be enabled and configured in order to collect data related to humidity, light, motion, and temperature.

For more information on enabling and configuring environmental sensor settings, see *environmental-sensor*.

NOTE
The environmental senor is supported only on an Brocade Mobility 1240 Access Point. When executed on any controller (other than an Brocade Mobility 1240 Access Point), the show > environmental-sensor > <parameters> command displays environmental-sensor details for adopted Brocade Mobility 1240 Access Points (if any).

Supported in the following platforms:

- Access Points — Brocade Mobility 1240 Access Point

Syntax:

```
show environmental-sensor
[history|humidity|light|motion|summary|temperature|version]

show environmental-sensor history {<1-HOUR>|<20-MINUTE>|<24-HOUR>}
show environmental-sensor [humidity|light|motion|summary|temperatue|version]
```

Parameters

```
show environmental-sensor history {<1-HOUR>|<20-MINUTE>|<24-HOUR>}
```

environmental-sensor history	Displays environmental sensor history once in every hour, 20 minutes, or 24 hours History includes the humidity, light, motion, and temperature data recorded by the sensor at specified time interval.
1-hour	Optional. Displays environmental sensor history once in every 1 (one) hour
20-minute	Optional. Displays environmental sensor history once in every 20 minutes
24-hour	Optional. Displays environmental sensor history once in every 24 hours

```
show environmental-sensor [humidity|light|motion|summary|temperatue|version]
```

environmental-sensor	Displays environmental sensor's recorded data, based on the parameters passed. The system displays the specified recorded data. The environmental sensor records data at the following intervals: 20 minutes, 1 hour, and 24 hours
humidity	Displays the minimum, average, and maximum humidity recorded
light	Displays the minimum, average, and maximum light recorded
motion	Displays the minimum, average, and maximum motion recorded:
temperature	Displays the minimum, average, and maximum temperature recorded
version	Displays the hardware and firmware versions
summary	Displays a summary of the data recorded at following intervals:

Example

```
ap8132-711728#show environmental-sensor summary
Maat Device uptime: 0 days 15:25:11
ERROR: Maat device is offline!
threshold polling-interval: 5
historical data polled 0 times per 2-minutes interval since Maat online

motion-sensor: Enabled(Demo)
  current value: 0 detected
  ------------------------------
               motion detected
  ------------------------------
  20-minute           0
```

```
  1-hour              0
  6-hour              0
  24-hour             0

temperature-sensor: Enabled(Demo)
  current value: -40.00 deg. C
  -------------------------------
               min/average/max
  -------------------------------
  20-minute         0/0/0
  1-hour            0/0/0
  6-hour            0/0/0
  24-hour           0/0/0

light-sensor: Enabled
  threshold-high:+400.00 threshold-low:+200.00 holdtime:11
  action radio-shutdown: radio-1 and radio-2
  light-on:1
  light-on/off event sent:0/0
  current value: 0.00 lux
  -------------------------------
               min/average/max
  -------------------------------
  20-minute         0/0/0
  1-hour            0/0/0
  6-hour            0/0/0
  24-hour           0/0/0

humidity-sensor: Enabled(Demo)
  current value: 0.00 %
  -------------------------------
               min/average/max
  -------------------------------
  20-minute         0/0/0
  1-hour            0/0/0
  6-hour            0/0/0
  24-hour           0/0/0
ap8132-711728#

ap8132-711634#show env-sensor history
Current Time: 2013-11-20 14:08:01 UTC
--------------------------------------------------------------------------------
---------------------
Sample-Interval          Motion           Temperature    Light
Humidity

-----------  min/average/max ---------------
--------------------------------------------------------------------------------
---------------------
20-minute                     1                         64/65/66
77/80                    58/60/61
1-hour                          24                      63/67/70
75/81                    57/59/61
6-hour                          128                     60/62/69
71/79                    52/56/71
24-hour                         188                     54/58/70
15/45                    49/57/73

ap8132-711634#
```

```
ap8132-711634#show env-sensor history 20-min
-------------------------------------------------------------------------------
------------------------------
timestamp                                       Motion
Temperature     Light                       Humidity
-------------------------------------------------------------------------------
------------------------------
2013-11-20 13:51:35 UTC           0                     66
79                            59
2013-11-20 13:53:35 UTC           0                     66
79                            59
2013-11-20 13:55:35 UTC           0                     65
79                            58
2013-11-20 13:57:35 UTC           1                     66
80                            59
2013-11-20 13:59:35 UTC           0                     66
79                            59
2013-11-20 14:02:35 UTC           0                     65
79                            60
2013-11-20 14:03:35 UTC           0                     64
79                            60
2013-11-20 14:05:35 UTC           2                     66
80                            60
2013-11-20 14:07:35 UTC           0                     66
80                            61
2013-11-20 14:09:35 UTC           0                     66
80                            61
ap8132-711634#

ap8132-711634#show env-sensor history 1-hr
-------------------------------------------------------------------------------
------------------------------
timestamp                                       Motion
Temperature     Light                       Humidity
-------------------------------------------------------------------------------
------------------------------
2013-11-20 13:51:35 UTC           0                     66
79                            59
2013-11-20 13:53:35 UTC           0                     66
79                            59
2013-11-20 13:55:35 UTC           0                     65
79                            58
2013-11-20 13:57:35 UTC           1                     66
80                            59
2013-11-20 13:59:35 UTC           0                     66
79                            59
2013-11-20 14:01:35 UTC           0                     65
79                            60
2013-11-20 14:03:35 UTC           0                     64
79                            60
2013-11-20 14:05:35 UTC           2                     66
80                            60
2013-11-20 14:07:35 UTC           0                     66
80                            61
2013-11-20 14:09:35 UTC           0                     66
80                            61
…
2013-11-20 14:42:35 UTC           0                     65
81                            60
```

```
2013-11-20 14:43:35 UTC           0                    64
80                          59
2013-11-20 14:45:35 UTC           3                    66
80                          60
2013-11-20 14:47:35 UTC           0                    66
81                          61
2013-11-20 14:49:35 UTC           0                    66
80                          61
ap8132-711634#

<DEVICE-NAME>#show env-sensor history 24-hr
------------------------------------------------------------------------------
------------------------------
timestamp                                        Motion
Temperature     Light                     Humidity
------------------------------------------------------------------------------
------------------------------
2013-11-20 10:10:20 UTC           27                   66
80                          60
2013-11-20 10:30:20 UTC           17                   66
80                          60
2013-11-20 10:50:20 UTC           17                   66
81                          60
2013-11-20 11:10:20 UTC           25                   66
81                          60
2013-11-20 11:30:20 UTC           24                   66
81                          60
2013-11-20 11:50:20 UTC           26                   66
81                          60

2013-11-21 08:10:20 UTC           9                    65
80                          59
2013-11-21 08:30:20 UTC           7                    65
80                          59
2013-11-21 08:50:20 UTC           12                   65
80                          60
2013-11-21 09:10:20 UTC           10                   65
80                          60
2013-11-21 09:30:20 UTC           15                   65
80                          60
2013-11-21 09:50:20 UTC           19                   66
80                          60
<DEVICE-NAME>#
```

event-history

show commands

Displays event history report

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show event-history {on <DEVICE-OR-DOMAIN-NAME>}
```

Parameters

```
show event-history {on <DEVICE-OR-DOMAIN-NAME>}
```

event-history	Displays event history report
on <DEVICE-OR-DOMAIN-NAME>	Optional. Displays event history report on a device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

Example

```
rfs4000-229D58(config)#show event-history on rfs4000-229D58
EVENT HISTORY REPORT
Generated on '2013-02-15 15:45:18 UTC' by 'admin'

2013-02-15 15:45:10     rfs4000-229D58  SYSTEM     LOGIN
Successfully logged in user 'admin' with privilege 'superuser' from 'ssh'
2013-02-15 15:45:01     rfs4000-229D58  SYSTEM     LOGOUT              Logged
out user 'admin' with privilege 'superuser' from '192.168.100.225'
2013-02-15 15:44:37     rfs4000-229D58  SYSTEM     LOGIN
Successfully logged in user 'admin' with privilege 'superuser' from 'ssh'
2013-02-15 15:44:16     rfs4000-229D58  SYSTEM     LOGOUT              Logged
out user 'admin' with privilege 'superuser' from '192.168.100.225'
2013-02-15 15:12:12     rfs4000-229D58  SYSTEM     LOGOUT              Logged
out user 'admin' with privilege 'superuser' from '192.168.100.224(web)'
2013-02-15 14:44:19     rfs4000-229D58  SYSTEM     CLOCK_RESET         System
clock reset, Time: 2013-02-15 14:45:30
rfs4000-229D58(config)#

nx4500-5CFA2B(config)#show event-history
EVENT HISTORY REPORT
Generated on '2013-04-10 14:53:21 UTC' by 'admin'

2013-04-10 14:22:16     nx4500-5CFA2B  SYSTEM     LOGIN
Successfully logged in user 'admin' with privilege 'superuser' from 'ssh'
2013-04-10 14:19:39     nx4500-5CFA2B  SYSTEM     LOGOUT            Logged out
user 'admin' with privilege 'superuser' from '192.168.100.222'
2013-04-10 12:45:46     nx4500-5CFA2B  SYSTEM     LOGIN
Successfully logged in user 'admin' with privilege 'superuser' from 'ssh'
2013-04-10 12:05:25  nx4500-5CFA2B DIAG   NEW_LED_STATE   LED state
2013-04-10 12:05:24  nx4500-5CFA2B DIAG   NEW_LED_STATE   LED state
message LED_LOCATIONING_OFF from module cfgd
2013-04-10 12:05:23     nx4500-5CFA2B  SYSTEM     SYSTEM_AUTOUP_ENABLE
Autoupgrade enabled for nx45xx
2013-04-10 12:05:23     nx4500-5CFA2B  SYSTEM     SYSTEM_AUTOUP_ENABLE
Autoupgrade enabled for nx65xx
2013-04-10 12:05:23     nx4500-5CFA2B  SYSTEM     SYSTEM_AUTOUP_ENABLE
Autoupgrade enabled for rfs4000
--More--
nx4500-5CFA2B(config)#
```

event-system-policy

show commands

Displays detailed event system policy configuration

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show event-system-policy [config|detail] <EVENT-SYSTEM-POLICY-NAME>
```

Parameters

```
show event-system-policy [config|detail] <EVENT-SYSTEM-POLICY-NAME>
```

event-system-policy	Displays event system policy configuration
config	Displays configuration for a specified policy
detail	Displays detailed configuration for a specified policy
<EVENT-SYSTEM-POLICY-NAME>	Specify the event system policy name.

Example

```
rfs7000-37FABE(config)#show event-system-policy config testpolicy
--------------------------------------------------------------------------------
MODULE          EVENT            SYSLOG    SNMP   FORWARD        EMAIL
--------------------------------------------------------------------------------
aaa       radius-discon-msg      on        on      on         default
--------------------------------------------------------------------------------
rfs7000-37FABE(config)#
```

file

show commands

Displays file system information

NOTE
This command is not available in the USER EXEC mode.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show file [information <FILE>|systems]
```

Parameters

```
show file [information <FILE>|systems]
```

information <FILE>	Displays file information • <FILE> – Specify the file name.
systems	Lists all file systems present in the system

Example

```
rfs7000-37FABE(config)#show file systems
File Systems:

     Size(b)     Free(b)     Type  Prefix
           -           -   opaque  system:
    10485760     9916416    flash  nvram:
    20971520    20131840    flash  flash:
           -           -  network  (null)
           -           -  network  rdp:
           -           -  network  sftp:
           -           -  network  http:
           -           -  network  ftp:
           -           -  network  tftp:
    20971520    20131840        -  hotspot:
rfs7000-37FABE(config)#
```

firewall

show commands

Displays wireless firewall information, such as *Dynamic Host Configuration Protocol* (DHCP) snoop table entries, denial of service statistics, active session summaries etc.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show firewall [dhcp|dos|flows]

show firewall [dhcp snoop-table|dos stats] {on <DEVICE-NAME>}

show firewall flows {filter|management|on|stats|wireless-client}

show firewall flows {filter} {(dir|dst port <1-65535>|ether|flow-type|icmp|
          igmp|ip|max-idle|min-bytes|min-idle|min-pkts|not|port|src|tcp|udp)}

show firewall flows {management {on <DEVICE-NAME>}|stats {on <DEVICE-NAME>}|
          wireless-client <MAC>|on <DEVICE-NAME>}
```

Parameters

`show firewall [dhcp snoop-table|dos stats] {on <DEVICE-NAME>}`

dhcp snoop-table	Displays DHCP snoop table entries • snoop-table – Displays DHCP snoop table entries DHCP snooping acts as a firewall between non-trusted hosts and the DHCP server. Snoop table entries contain MAC address, IP address, lease time, binding type, and interface information of non-trusted interfaces.
dos stats	Displays *Denial of Service* (DoS) statistics This option is not available in the User Exec mode.
on <DEVICE-NAME>	The following keyword is common to the 'DHCP snoop table' and 'DoS stats' parameters: • on <DEVICE-NAME> – Optional. Displays snoop table entries, or DoS stats on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`show firewall flows {filter} {(dir|dst|ether|flow-type|icmp|igmp|ip|max-idle|min-bytes|min-idle|min-pkts|not|port|src|tcp|udp)}`

firewall flows	Notifies a session has been established
filter	Optional. Defines additional firewall flow filter parameters
dir [wired-wired| wired-wireless| wireless-wired| wireless-wireless]	Optional. Matches the packet flow direction • wired-wired – Wired to wired flows • wired-wireless – Wired to wireless flows • wireless-wired – Wireless to wired flows • wireless-wireless – Wireless to wireless flows
dst port <1-65535>	Optional. Matches the destination port with the specified port • port <1-65535> – Specifies the destination port number from 1 - 65535
ether [dst <MAC>| host <MAC>| src <MAC>| vlan <1-4094>]	Optional. Displays Ethernet filter options • dst <MAC> – Matches only the destination MAC address • host <MAC> – Matches flows containing the specified MAC address • src <MAC> – Matches only the source MAC address • vlan <1-4094> – Matches the VLAN number of the traffic with the specified value. Specify a value from 1- 4094.
flow-type [bridged|natted|routed| wired|wireless]	Optional. Matches the traffic flow type • bridged – Bridged flows • natted – Natted flows • routed – Routed flows • wired – Flows belonging to wired hosts • wireless – Flows containing a mobile unit
icmp {code|type}	Optional. Matches flows with the specified *Internet Control Message Protocol* (ICMP) code and type • code – Matches flows with the specified ICMP code • type – Matches flows with the specified ICMP type
igmp	Optional.Matches *Internet Group Management Protocol* (IGMP) flows
ip [dst <IP>| host <IP>| proto <0-254>| src <IP>]	Optional. Filters firewall flows based on the IPv4 parameters passed • dst <IP> – Matches destination IP address • host <IP> – Matches flows containing IPv4 address • proto <0-254> – Matches the IPv4 protocol number with the specified number • src <IPv4> – Matches source IP address
max-idle <1-4294967295>	Optional. Filters firewall flows idle for at least the specified duration. Specify a max-idle value from 1 - 4294967295 bytes.
min-bytes <1-4294967295>	Optional. Filters firewall flows with at least the specified number of bytes. Specify a min-bytes value from 1 - 4294967295 bytes.

min-idle <1-4294967295>	Optional. Filters firewall flows idle for at least the specified duration. Specify a min-idle value from 1 - 4294967295 bytes.
min-pkts <1-4294967295>	Optional. Filters firewall flows with at least the given number of packets. Specify a min-bytes value from 1 - 4294967295 bytes.
not	Optional. Negates the filter expression selected
port <1-65535>	Optional. Matches either the source or destination port. Specify a port from 1 - 65535.
src <1-65535>	Optional. Matches only the source port with the specified port. Specify a port from 1 - 65535.
tcp	Optional. Matches TCP flows
udp	Optional. Matches UDP flows

`show firewall flows {management {on <DEVICE-NAME>}|stats {on <DEVICE-NAME>}| wireless-client <MAC>|on <DEVICE-NAME>}`

firewall flows	Notifies a session has been established
management {on <DEVICE-NAME>}	Optional. Displays management traffic firewall flows • on <DEVICE-NAME> – Optional. Displays firewall flows on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.
stats {on <DEVICE-NAME>}	Optional. Displays active session summary • on <DEVICE-NAME> – Optional. Displays active session summary on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.
wireless-client <MAC>	Optional. Displays wireless clients firewall flows • <MAC> – Specify the MAC address of the wireless client.
on <DEVICE-NAME>	Optional. Displays all firewall flows on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Example

```
rfs7000-37FABE(config)#show firewall dhcp snoop-table on rfs7000-37FABE
Snoop Binding <157.235.208.252, 00-15-70-37-FA-BE, Vlan 4>
Type Controller-SVI, Touched 32 seconds ago
------------------------------------------------------------------------------
Snoop Binding <172.16.10.2, 00-15-70-37-FA-BE, Vlan 1>
Type Controller-SVI, Touched 1 seconds ago
------------------------------------------------------------------------------
rfs7000-37FABE(config)#


rfs7000-37FABE(config)#show firewall flows management on rfs7000-37FABE
========== Flow# 1 Summary ==========
Forward:
 Vlan 1, TCP 172.16.10.10 port 3995 > 172.16.10.1 port 22
 00-02-B3-28-D1-55 > 00-15-70-37-FA-BE, ingress port ge1
 Egress port: <local>, Egress interface: vlan1, Next hop: <local>
(00-15-70-37-FA-BE)
 573 packets, 49202 bytes, last packet 0 seconds ago
Reverse:
 Vlan 1, TCP 172.16.10.1 port 22 > 172.16.10.10 port 3995
 00-15-70-37-FA-BE > 00-02-B3-28-D1-55, ingress port local
 Egress port: ge1, Egress interface: vlan1, Next hop: 172.16.10.10
(00-02-B3-28-D1-55)
 552 packets, 63541 bytes, last packet 0 seconds ago
TCP state: Established
Flow times out in 1 hour 30 minutes
```

```
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show firewall flows stats on rfs7000-37FABE
Active Flows       2
TCP flows          1
UDP flows          0
DHCP flows         1
ICMP flows         0
IPsec flows        0
L3/Unknown flows   0
rfs7000-37FABE(config)#
```

global

show commands

Displays global information for network devices based on the parameters passed

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show global [device-list|domain]

show global device-list {filter {offline|online|rf-domain}}
show global device-list {filter {offline|online}}
show global device-list {filter rf-domain [<DOMAIN-NAME>|not <DOMAIN-NAME>]}

show global domain managers
```

Parameters

```
show global device-list filter {offline|online}
```

global device-list	Displays global information for all network devices. Use the following keywords to specify additional filters: offline, online, and rf-domain.
filter {offline|online}	Optional. Specifies additional filters • offline – Optional. Displays global information for offline devices only • online – Optional. Displays global information for online devices only

	`show global device-list filter` *(rf-domain [<DOMAIN-NAME>|not <DOMAIN-NAME>])*
global device-list	Displays global information for all network devices. Use the following keywords to specify additional filters: offline, online, and rf-domain.
filter rf-domain [<DOMAIN-NAME>| not <DOMAIN-NAME>]	Optional. Specifies additional filters • rf-domain – Optional. Displays global information for all devices in a specified RF Domain • <DOMAIN-NAME> – Optional. Displays information of all devices within the domain identified by the <DOMAIN-NAME> keyword • not <DOMAIN-NAME> – Optional. Displays information of all devices in domains not matching the <DOMAIN-NAME> keyword

	`show global domain managers`
global domain managers	Displays global information for all RF Domains and managers in the network

Example

```
rfs4000-229D58#show global device-list
-------------------------------------------------------------------------------
---------------------------------
             MAC     HOST-NAME      TYPE         CLUSTER       RF-DOMAIN
ADOPTED-BY     ONLINE
-------------------------------------------------------------------------------
---------------------------------
 00-23-68-22-9D-58  rfs4000-229D58 rfs4000                default
online
-------------------------------------------------------------------------------
---------------------------------
Total number of clients displayed: 1
rfs4000-229D58#

rfs4000-229D58#show global device-list filter rf-domain default
-------------------------------------------------------------------------------
---------------------------------
             MAC     HOST-NAME      TYPE         CLUSTER       RF-DOMAIN
ADOPTED-BY     ONLINE
-------------------------------------------------------------------------------
---------------------------------
 00-23-68-22-9D-58  rfs4000-229D58 rfs4000                default
online
-------------------------------------------------------------------------------
---------------------------------
Total number of clients displayed: 1
rfs4000-229D58#

rfs4000-229D58#show global domain managers
-------------------------------------------------------------------------------
---
           RF-DOMAIN               MANAGER             HOST-NAME     APS CLIENTS
-------------------------------------------------------------------------------
---
             default     00-23-68-22-9D-58        rfs4000-229D58       1       0
-------------------------------------------------------------------------------
---
Total number of RF-domain displayed: 1
rfs4000-229D58#
```

gre

show commands

Displays GRE tunnel info

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show gre info
```

Parameters

```
show gre info
```

show gre info	Displays *Generic Routing Encapsulation* (GRE) information.

Example

```
nx4500-5CFA2B>show gre info
Gre Tunnel info:
    {'No tunnel found': 0}
nx4500-5CFA2B>
```

interface

show commands

Displays configured system interfaces and their status

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show interface
{<INTERFACE-NAME>|brief|counters|ge|me1|on|port-channel|pppoe1|
          switchport|vlan|wwan1}
show interface {<INTERFACE-NAME>|brief|counters|ge <1-4>|me1|on|port-channel
<1-2>|
          pppoe1|switchport|vlan <1-4094>|wwan1} {on <DEVICE-NAME>}
```

Parameters

```
show interface {<INTERFACE-NAME>|brief|counters|ge <1-4>|me1|on|port-channel
<1-2>|
pppoe1|switchport|vlan <1-4094>|wwan1} {on <DEVICE-NAME>}
```

interfaces	Optional. Displays system interface status based on the parameters passed
<INTERFACE-NAME>	Optional. Displays status of the interface specified by the <INTERFACE-NAME> parameter. Specify the interface name.
brief	Optional. Displays a brief summary of the interface status and configuration
counters	Optional. Displays interface Tx or Rx counters
ge <1-4>	Optional. Displays Gigabit Ethernet interface status and configuration • <1-4> – Select the Gigabit Ethernet interface index from 1 - 4.
me1	Optional. Displays Fast Ethernet interface status and configuration
port-channel <1-2>	Optional. Displays port channel interface status and configuration • <1-2> – Specify the port channel index from 1 - 2.
pppoe1	Optional. Displays PPP over Ethernet interface status and configuration
switch port	Optional. Displays layer 2 interface status
vlan <1-4094>	Optional. Displays VLAN interface status and configuration • <1-4094> – Specify the *Switch Virtual Interface* (SVI) VLAN ID from 1 - 4094.
wwan1	Optional. Displays Wireless WAN interface status, configuration, and counters
on <DEVICE-NAME>	The following keywords are common to all of the above interfaces: • on <DEVICE-NAME> – Optional. Displays interface related information on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Example

```
Following are the interfaces available on a Brocade Mobility 71XX Access Point
controller:

rfs7000-37FABE(config)#show interface ?
  WORD          Interface name
  brief         Brief summary of interface status and configuration
  counters      Interface tx/rx counters
  ge            GigabitEthernet interface
  me1           FastEthernet interface
  on            On AP/Controller
  port-channel  Port-Channel interface
  pppoe1        PPP Over Ethernet interface
  switchport    Status of Layer2 interfaces
  vlan          Switch VLAN interface
  wwan1         Wireless WAN interface
  |             Output modifiers
  >             Output redirection
  >>            Output redirection appending
  <cr>

rfs7000-37FABE(config)#


nx4500-5CFA2B(config)#

rfs7000-37FABE(config)#show interface switchport on rfs7000-37FABE
-------------------------------------------------------------------------------
----------
 INTERFACE          STATUS   MODE     VLAN(S)
```

```
--------------------------------------------------------------------------------
----------
 ge1               UP       access   1
 ge2               UP       access   1
 ge3               UP       access   1
 ge4               UP       access   1
--------------------------------------------------------------------------------
----------
A '*' next to the VLAN ID indicates the native vlan for that trunk port
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show interface vlan 1
Interface vlan1 is UP
  Hardware-type: vlan, Mode: Layer 3, Address: 00-15-70-37-FA-BE
  Index: 4, Metric: 1, MTU: 1500
  IP-Address: 172.16.10.1/24
    input packets 587971, bytes 58545041, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 56223, bytes 4995566, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show interface ge 2 on rfs7000-37FABE
Interface ge2 is DOWN
  Hardware-type: ethernet, Mode: Layer 2, Address: 00-15-70-37-FA-C0
  Index: 2002, Metric: 1, MTU: 1500
  Speed: Admin Auto, Operational n/a, Maximum 1G
  Duplex: Admin Auto, Operational n/a
  Active-medium: n/a
  Switchport settings: access, access-vlan: 1
    Input packets 0, bytes 0, dropped 0
    Received 0 unicasts, 0 broadcasts, 0 multicasts
    Input errors 0, runts 0, giants 0
    CRC 0, frame 0, fragment 0, jabber 0
    Output packets 501587, bytes 60935912, dropped 0
    Sent 3 unicasts, 4613 broadcasts, 496971 multicasts
    Output errors 0, collisions 0, late collisions 0
    Excessive collisions 0

rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show interface counters
--------------------------------------------------------------------------------
---------------------------------
    #       MAC       RX-PKTS       RX-BYTES       RX-DROP       TX-PKTS
TX-BYTES         TX-DROP
--------------------------------------------------------------------------------
---------------------------------
 me1    00-...-F7 0           0            0           0           0
0
 vlan1   00-...-BE 353854        57627570       0             126392
37379394       0
 ge1     00-...-BF 299841        32267476       0             117557
41052744       0
 ge2     00-...-C0 0             0              0             274490
30705325       0
 ge3     00-...-C1 0             0              0             274490
30705325       0
```

```
 ge4     00-...-C2 0             0              0             274490
30705325       0
-------------------------------------------------------------------------------
----------
rfs7000-37FABE(config)#


nx6500-31FABE(config)#show interface switchport on nx6500-31FABEE
-------------------------------------------------------------------------------
 INTERFACE          STATUS   MODE     VLAN(S)
-------------------------------------------------------------------------------
 ge1                UP       access   1
 ge2                DOWN     access   1
 -------------------------------------------------------------------------------
A '*' next to the VLAN ID indicates the native vlan for that trunk port
nx6500-31FABE(config)#

nx6500-31FABE(config)#show interface vlan 1
Interface vlan1 is UP
  Hardware-type: vlan, Mode: Layer 3, Address: 00-15-70-37-FA-BE
  Index: 4, Metric: 1, MTU: 1500
  IP-Address: 172.16.10.1/24
    input packets 587971, bytes 58545041, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 56223, bytes 4995566, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
nx6500-31FABE(config)#

nx6500-31FABE(config)#show interface ge 2 on nx6500-31FABE
Interface ge2 is DOWN
  Hardware-type: ethernet, Mode: Layer 2, Address: 00-15-70-37-FA-C0
  Index: 2002, Metric: 1, MTU: 1500
  Speed: Admin Auto, Operational n/a, Maximum 1G
  Duplex: Admin Auto, Operational n/a
  Active-medium: n/a
  Switchport settings: access, access-vlan: 1
    Input packets 0, bytes 0, dropped 0
    Received 0 unicasts, 0 broadcasts, 0 multicasts
    Input errors 0, runts 0, giants 0
    CRC 0, frame 0, fragment 0, jabber 0
    Output packets 501587, bytes 60935912, dropped 0
    Sent 3 unicasts, 4613 broadcasts, 496971 multicasts
    Output errors 0, collisions 0, late collisions 0
    Excessive collisions 0

nx6500-31FABE(config)#

nx6500-31FABE(config)#show interface counters
-------------------------------------------------------------------------------
    #       MAC       RX-PKTS       RX-BYTES       RX-DROP       TX-PKTS
TX-BYTES         TX-DROP
-------------------------------------------------------------------------------
 vlan1   00-...-BE 588384        58580154       0             56435
5013682        0
 ge1     00-...-BF 1906950       175560930      0             1402226
589235764      0
 ge2     00-...-C0 0             0              0             501615
60939303       0
-------------------------------------------------------------------------------
```

```
nx6500-31FABE(config)#
```

ip

show commands

Displays IP related information

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show ip [arp|ddns|default-gateways|dhcp|dhcp-vendor-options|domain-name|igmp|
          interface|name-server|nat|ospf|route|routing]

show ip arp {<VLAN-NAME>} {(on <DEVICE-NAME>)}

show ip ddns bindings {on <DEVICE-NAME>}

show ip dhcp [binding|networks|status]
show ip dhcp binding {manual} {(on <DEVICE-NAME>)}
show ip dhcp [networks|status] {on <DEVICE-NAME>}

show ip
[default-gateways|dhcp-vendor-options|domain-name|name-server|routing]
          {on <DEVICE-NAME>}

show ip igmp snooping [mrouter|vlan]
show ip igmp snooping mrouter vlan <1-4095> {on <DEVICE-NAME>}
show ip igmp snooping vlan <1-4095> {<IP>} {(on <DEVICE-NAME>)}

show ip interface {<INTERFACE-NAME>|brief|on}
show ip interface {<INTERFACE-NAME>|brief} {(on <DEVICE-NAME>)}

show ip nat translations verbose {on <DEVICE-NAME>}

show ip route {<INTERFACE-NAME>|ge|me1|on|port-channel|pppoe1|vlan|wwan1}
show ip route {<INTERFACE-NAME>|ge <1-4>|me1|port-channel <1-2>|vlan <1-4094>|
          pppoe1|wwan1} {(on <DEVICE-NAME>)}

show ip ospf {border-router|interface|neighbor|on|route|state}
show ip ospf {border-router|neighbor|route|on|state} {on <DEVICE-NAME>}
show ip ospf {interface} {vlan|on}
show ip ospf {interface} {vlan <1-4094>} {(on <DEVICE-NAME>)}
```

NOTE
The show ip ospf command is also available under the ‘profile’ and ‘device’ modes.

Parameters

`show ip arp {<VLAN-NAME>} {(on <DEVICE-NAME>)}`

ip arp	Displays *Address Resolution Protocol* (ARP) mappings
<VLAN-NAME>	Optional. Displays ARP mapping on a specified VLAN. Specify the VLAN name.
on <DEVICE-NAME>	The following keyword is recursive and common to the 'vlan-name' parameter: • on <DEVICE-NAME> – Optional. Displays ARP configuration details on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`show ip ddns bindings {on <DEVICE-NAME>}`

ip ddns	Displays *Dynamic Domain Name Server* (DDNS) configuration details
bindings {on <DEVICE-NAME>}	Displays DDNS address bindings • on <DEVICE-NAME> – Optional. Displays address bindings on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`show ip dhcp [networks|status] {on <DEVICE-NAME>}`

ip dhcp	Displays DHCP server related details, such as network and status
networks	Displays DHCP server network details
status	Displays DHCP server status
on <DEVICE-NAME>	The following keyword is common to all of the above parameters: • on <DEVICE-NAME> – Optional. Displays server status and network details on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`show ip dhcp binding {manual} {(on <DEVICE-NAME>)}`

ip dhcp	Displays the DHCP server configuration details
bindings	Displays DHCP address bindings
manual	Displays static DHCP address bindings
on <DEVICE-NAME>	The following keyword is recursive and common to the 'manual' parameter: • on <DEVICE-NAME> – Optional. Displays DHCP address bindings on a specified device • <DEVICE-NAME> – Optional. Specify the name of the AP, wireless controller, or service platform.

`show ip [default-gateways|dhcp-vendor-options|domain-name|name-server|routing] {on <DEVICE-NAME>}`

ip default-gateways	Displays all learnt default gateways
ip dhcp-vendor-options	Displays DHCP 43 parameters received from the DHCP server. This output includes the interface from which the option was learned.
ip domain-name	Displays the DNS default domain
ip name-server	Displays the DNS name server details
ip routing	Displays routing status
on <DEVICE-NAME>	The following keywords are common to all of the above parameters: • on <DEVICE-NAME> – Optional. Displays IP related information, based on the parameters passed, on a specified device • <DEVICE-NAME> – Optional. Specify the name of the AP, wireless controller, or service platform.

`show ip igmp snooping mrouter vlan <1-4095> {on <DEVICE-NAME>}`

ip igmp snooping	Displays the IGMP snooping configuration

mrouter	Displays the IGMP snooping multicast router (mrouter) configuration
vlan <1-4095> {on <DEVICE-NAME>}	Displays the IGMP snooping multicast router configuration for a VLAN • <1-4095> – Specify the VLAN ID from 1 - 4095. • on <DEVICE-NAME> – Optional. Displays the IGMP snooping mrouter configuration on a specified device • <DEVICE-NAME> – Specify the name of the AP or wireless controller.

`show ip igmp snooping vlan <1-4095> {<IP>} {(on <DEVICE-NAME>)}`

ip igmp snooping	Displays the IGMP snooping configuration
vlan <1-4095>	Displays the VLAN IGMP snooping configuration • <1-4095> – Specify the VLAN ID from 1 - 4095.
<IP>	Optional. Specifies the multicast group IP address
on <DEVICE-NAME>	The following keyword is recursive and common to the 'ip' parameter: • on <DEVICE-NAME> – Optional. Displays configuration details on a specified device • <DEVICE-NAME> – Specify the name of the AP or wireless controller.

`show ip interface {<INTERFACE-NAME>|brief} {(on <DEVICE-NAME>)}`

ip interface	Displays an administrative and operational status of all layer 3 interfaces or a specified layer 3 interface
<INTERFACE-NAME>	Displays a specified interface status. Specify the interface name.
brief	Displays a brief summary of all interface status and configuration
on <DEVICE-NAME>	The following keyword is recursive and common to the 'interface-name' and 'brief' parameters: • on <DEVICE-NAME> – Optional. Displays interface status and summary, based on the parameters passed, on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`show ip nat translations verbose {on <DEVICE-NAME>}`

ip nat translations	Displays *Network Address Translation* (NAT) translations
verbose	Displays detailed NAT translations • on <DEVICE-NAME> – Optional.Displays NAT translations on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`show ip route {<INTERFACE-NAME>|ge <1-4>|me1|port-channel <1-2>|vlan <1-4094>|pppoe1|wwan1} {(on <DEVICE-NAME>)}`

ip route	Displays route table details. The route tables use flags to distinguish between routes. The different flags are: • C – Connected • G – Gateway • O – OSPF route • S – Static route **NOTE:** Flags 'S' and 'O' identify static learned routes and dynamic learned routes respectively.
<INTERFACE-NAME>	Displays route table details for a specified interface. Specify the interface name
ge <1-4>	Displays GigabitEthernet interface route table details • <1-4> – Specify the GigabitEthernet interface index from 1 - 4.
me1	Displays FastEthernet interface route table details
port-channel <1-2>	Displays port channel interface route table details. Specify the port channel index from 1 - 2.
vlan <1-4095>	Displays VLAN interface route table details. Select the VLAN interface ID from 1 - 4094.

pppoe1	Displays *Point-to-point Protocol over Ethernet* (PPPoE) interface route table details
wwan1	Displays Wireless WAN route table details
on <DEVICE-NAME>	The following keywords are recursive and common to all of the above parameters: • on <DEVICE-NAME> – Displays route table details, based on the parameters passed, on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`show ip ospf {border-router|interface|neighbor|route|on|state} {on <DEVICE-NAME>}`

ip ospf	Displays overall OSPF information
border-router	Optional. Displays details of all the border routers connected
interface {on| vlan <1-4094>} {on <DEVICE-NAME>}	Optional. Displays details of all the interfaces with OSPF enabled • on <DEVICE-NAME> – Optional. Displays specified device details • vlan <1-4094> – Displays VLAN interface details • <DEVICE-NAME> – Specify the name of the AP or wireless controller.
neighbor	Optional. Displays an OSPF neighbors list
route	Optional. Displays OFPS routes information
state	Optional. Displays an OSPF process state
on <DEVICE-NAME>	The following keywords are recursive and common to all of the above parameters: • on <DEVICE-NAME> – Optional. Displays overall OSPF information, based on the parameters passed, on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Example

```
rfs7000-37FABE(config)#show ip arp on rfs7000-37FABE
------------------------------------------------------------------------------
---
          IP                      MAC               INTERFACE          TYPE
------------------------------------------------------------------------------
---
  172.16.10.12         5C-D9-98-4C-04-51         vlan1           dynamic
  172.16.10.4          00-15-70-38-06-49         vlan1           dynamic
------------------------------------------------------------------------------
---
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show ip interface brief on rfs7000-37FABE
------------------------------------------------------------------------------
--
 INTERFACE          IP-ADDRESS/MASK            TYPE        STATUS    PROTOCOL
------------------------------------------------------------------------------
--
 me1                192.168.0.1/24             primary     UP        down
 vlan1              172.16.10.1/24             primary     UP        up
------------------------------------------------------------------------------
--
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show ip route test on rfs7000-37FABE
+-------------------------+--------------------+------------+-------------
|       DESTINATION       |      GATEWAY       |   FLAGS    |    INTERFACE     |
+-------------------------+--------------------+------------+-------------
| 157.235.208.0/24        | direct             | C          | vlan4            |
```

```
| 172.16.10.0/24          | direct             | C          | vlan1           |
| default                 | 172.16.10.9        | CG         | vlan1           |
+-------------------------+--------------------+------------+-------------
Flags:  C - Connected G - Gateway
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show ip route pc on rfs7000-37FABE
--------------------------------------------------------------------------------
---
        DESTINATION             GATEWAY          FLAGS           INTERFACE
--------------------------------------------------------------------------------
---
  192.168.0.0/24            direct            C              me1
  172.16.10.0/24            direct            C              vlan1
--------------------------------------------------------------------------------
---
Flags:  C - Connected G - Gateway
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show ip route vlan 1 on rfs7000-37FABE
+-------------------------+--------------------+-------------+------------
|      DESTINATION        |       GATEWAY      |    FLAGS    |    INTERFACE    |
+-------------------------+--------------------+-------------+------------
| 172.16.10.0/24          | direct             | C           | vlan1           |
| default                 | 172.16.10.9        | CG          | vlan1           |
+-------------------------+--------------------+-------------+------------
Flags:  C - Connected G - Gateway
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show ip route ge 1 on rfs7000-37FABE
--------------------------------------------------------------------------------
   DESTINATION             GATEWAY          FLAGS           INTERFACE
--------------------------------------------------------------------------------
  172.16.12.0/24            direct            C              vlan3
  172.16.11.0/24            direct            C              vlan2
  172.16.10.0/24            direct            C              vlan1
--------------------------------------------------------------------------------
Flags:  C - Connected G - Gateway
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show ip routing on rfs7000-37FABE
IP routing is enabled.
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show ip dhcp status on rfs7000-37FABE
State of DHCP server: running
Interfaces: vlan2, vlan3
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show ip ospf state on rfs7000-37FABE
 Maximum number of OSPF routes allowed: 9216
   Number of OSPF routes received: 0
   Ignore-count allowed: 5, current ingore-count: 0
   Ignore-time 60 seconds, reset-time 360 seconds
   Current OSPF process state: Running
rfs7000-37FABE(config)#

rfs7000-37FABE#show ip route vlan 1
--------------------------------------------------------------------------------
---
```

```
        DESTINATION             GATEWAY          FLAGS           INTERFACE
-------------------------------------------------------------------------------
---
  172.16.10.0/24            direct            C              vlan1
-------------------------------------------------------------------------------
---
Flags:  C - Connected G - Gateway O - OSPF S - Static
rfs7000-37FABE#

rfs4000-882A17#show ip route on br7131-0B863C
-------------------------------------------------------------------------------
---
       DESTINATION             GATEWAY          FLAGS          INTERFACE
-------------------------------------------------------------------------------
---
  192.168.9.0/24          192.168.0.12          O           vlan10
  192.168.0.0/24          direct                C           vlan10
  192.168.5.0/24          192.168.0.12          O           vlan10
  192.168.6.0/24          192.168.0.12          O           vlan10
  172.20.15.0/24          direct                C           vlan66
  99.99.99.96/32          192.168.0.53          S           vlan10
  99.99.99.97/32          192.168.0.40          S           vlan10
-------------------------------------------------------------------------------
---
Flags:  C - Connected G - Gateway O - OSPF S - Static
rfs4000-882A17#

nx6500-31FABE(config)#show ip route ge 1 on nx6500-31FABE
-------------------------------------------------------------------------------
   DESTINATION             GATEWAY          FLAGS           INTERFACE
-------------------------------------------------------------------------------
  172.16.12.0/24            direct            C              vlan3
  172.16.11.0/24            direct            C              vlan2
  172.16.10.0/24            direct            C              vlan1
-------------------------------------------------------------------------------
Flags:  C - Connected G - Gateway
nx6500-31FABE(config)#

nx6500-31FABE(config)#show ip routing on nx6500-31FABE
IP routing is enabled.
nx6500-31FABE(config)#

nx6500-31FABE(config)#show ip dhcp status on nx6500-31FABE
State of DHCP server: running
Interfaces: vlan2, vlan3
nx6500-31FABE(config)#

rfs4000-229D58#show ip dhcp-vendor-options
-------------------------------------------------------------------------------
---
                ITEM                        VALUE             INTERFACE
-------------------------------------------------------------------------------
---
  Server Info                       n/a                   vlan400
  Firmware Image File               n/a                   vlan400
  Config File                       n/a                   vlan400
  Legacy Adoption Info              192.168.30.1          vlan300
  AP Adoption Info                  192.168.50.2          vlan500
  AP Adoption Info                  192.168.50.3          vlan500
  Controller Adoption Info          n/a                   n/a
```

```
-------------------------------------------------------------------------------
---
rfs4000-229D58#
```

ip-access-list

show commands

Displays IP access list statistics

NOTE
This command is not available in the USER EXEC Mode.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show ip-access-list stats {<IP-ACCESS-LIST-NAME>|detail|on}
show ip-access-list stats {<IP-ACCESS-LIST-NAME>|detail <IP-ACCESS-LIST-NAME>}
          {(on <DEVICE-NAME>)}
```

Parameters

```
show ip-access-list stats {<IP-ACCESS-LIST-NAME>|detail <IP-ACCESS-LIST-NAME>}
       {(on <DEVICE-NAME>)}
```

ip-access-list stats	Displays IP access list statistics
<IP-ACCESS-LIST-NAME>	Optional. Displays statistics for a specified IP access list. Specify the IP access list name.
detail <IP-ACCESS-LIST-NAME>	Optional. Displays detailed statistics for a specified IP access list. Specify the IP access list name.
on <DEVICE-NAME>	The following keyword is recursive and common to the 'IP-ACCESS-LIST-NAME' and 'detail' parameters: • on <DEVICE-NAME> – Optional. Displays all or a specified IP access list statistics on a specified device. • <DEVICE-NAME> – Optional. Specify the name of the AP, wireless controller, or service platform.

Example

```
rfs7000-37FABE(config)#show ip-access-list stats
IP Access-list: # Restrict Management ACL #
  permit tcp any any eq ftp rule-precedence 1        Hitcount: 0
  permit tcp any any eq www rule-precedence 2        Hitcount: 4
  permit tcp any any eq ssh rule-precedence 3        Hitcount: 448
  permit tcp any any eq https rule-precedence 4        Hitcount: 0
  permit udp any any eq snmp rule-precedence 5       Hitcount: 0
  permit tcp any any eq telnet rule-precedence 6       Hitcount: 4
rfs7000-37FABE(config)#

The following example displays the 'auto-tunnel-acl' IP ACL configuration:

rfs4000-229D58(config)#ip access-list auto-tunnel-acl
```

```
rfs4000-229D58(config-ip-acl-auto-tunnel-acl)#show context
ip access-list auto-tunnel-acl
permit ip host 200.200.200.99 30.30.30.1/24 rule-precedence 2
permit ip host 200.200.200.99 any rule-precedence 3
rfs4000-229D58(config-ip-acl-auto-tunnel-acl)#
```

The following example dispalys the statistics for the ‘auto-tunnel-acl’ ACL:

```
rfs4000-229D58#show ip-access-list stats
IP Access-list: auto-tunnel-acl
  permit ip host 200.200.200.99 30.30.30.1/24 rule-precedence 2
Hitcount: 0
  permit ip host 200.200.200.99 any rule-precedence 3        Hitcount: 0

rfs4000-229D58#

nx6524-5483B0#show ip-access-list stats scaleacl | i 125
  permit ip host 125.1.1.1 any rule-precedence 125        Hitcount: 893
Hardware Hitcount: 3120
  permit ip host 125.2.1.1 any rule-precedence 346         Hitcount: 0
Hardware Hitcount: 0
nx6524-5483B0#
```

l2tpv3

show commands

Displays a *Layer 2 Tunnel Protocol Version 3 (L2TPV3)* session information

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
l2tpv3 {on|tunnel|tunnel-summary}

l2tpv3 {on <DEVICE-NAME>}

l2tpv3 {tunnel <L2TPV3-TUNNEL-NAME>} {session <L2TPV3-SESSION-NAME>}
          {(on <DEVICE-NAME>)}

l2tpv3 {tunnel-summary} {down|on|up}
l2tpv3 {tunnel-summary} {on <DEVICE-NAME>}
l2tpv3 {tunnel-summary} {down|up} {on <DEVICE-NAME>}
```

Parameters

	`l2tpv3 {on <DEVICE-NAME>}`
l2tpv3 {on <DEVICE-NAME>}	Displays a L2TPv3 tunnel and session details or summary • on <DEVICE-NAME> – Optional. Displays L2TPv3 information on a specified access point or wireless controller • <DEVICE-NAME> – Specify the name of AP, wireless controller, or service platform.

	`l2tpv3 {tunnel <L2TPV3-TUNNEL-NAME>} {session <L2TPV3-SESSION-NAME>} {(on <DEVICE-NAME>)}`
l2tpv3	Displays a L2TPv3 tunnel and session details or summary
tunnel <L2TPV3-TUNNEL-NAME>	Optional. Displays a specified L2TPv3 tunnel information • <L2TPV3-TUNNEL-NAME> – Specify the L2TPv3 tunnel name.
session <L2TPV3-SESSION-NAME>	Optional. Displays a specified L2TPv3 tunnel session information • <L2TPV3-SESSION-NAME> – Specify the session name.
on <DEVICE-NAME>	The following keyword is recursive and common to the 'session <L2TPV3-SESSION-NAME>' parameter. • on <DEVICE-NAME> – Optional. Displays a L2TPv3 tunnel and session details, based on the parameters passed, on a specified device. • <DEVICE-NAME> – Specify the name of AP, wireless controller, or service platform.

	`l2tpv3 {tunnel-summary} {on <DEVICE-NAME>}`
l2tpv3	Displays L2TPv3 tunnel and session details or summary For an L2TPv3 tunnel over Auto IPSec, the tunnel status is displayed as: Established (secured by ipsec)
tunnel-summary {on <DEVICE-NAME>}	Optional. Displays L2TPv3 tunnel summary • on <DEVICE-NAME> – Optional. Displays a L2TPv3 tunnel summary on a specified device • <DEVICE-NAME> – Specify the name of AP, wireless controller, or service platform.

	`l2tpv3 {tunnel-summary} {down|up} {on <DEVICE-NAME>}`
l2tpv3	Displays a L2TPv3 tunnel and session details or summary
tunnel-summary	Optional. Displays a L2TPv3 tunnel summary, based on the parameters passed
down	Optional. Displays un-established tunnels summary
up	Optional. Displays established tunnels summary
on <DEVICE-NAME>	The following keyword is common to the 'down' and 'up' parameters: • on <DEVICE-NAME> – Optional. Displays summary, for un-established or established tunnels, on a specified device • <DEVICE-NAME> – Specify the name of AP, wireless controller, or service platform.

Example

```
ap7131-11E6C4#show l2tpv3 tunnel-summary
-------------------------------------------------------------------------------
----------
Sl No  Tunnel Name      Tunnel State            Estd/Total  Sessions
Encapsulation Protocol
-------------------------------------------------------------------------------
----------
1      testTunnel     Established (secured by ipsec)       1/1             IP
Total Number of Tunnels 1
ap7131-11E6C4#

ap7131-11E6C4#show l2tpv3
-------------------------------------------------------------------------------
--
Tunnel Name : testTunnel
```

```
  Control connection id : 2238970979
  Peer Address : 30.1.1.1
  Local Address : 30.1.1.30
  Encapsulation Protocol : IP
  MTU : 1460
  Peer Host Name : rfss
  Peer Vendor Name : Brocade
  Peer Control Connection ID : 322606389
  Tunnel State : Established (secured by ipsec)
  Establishment Criteria : always
  Sequence number of the next msg to the peer : 29
  Expected sequence number of the next msg from the peer :42
  Sequence number of the next msg expected by the peer : 29
  Retransmission count : 0
  Reconnection count : 0
  Uptime : 0 days 1 hours 2 minutes 47 seconds

-------------------------------------------------------------------------
--
  Session Name : session1
    VLANs : 30
    Pseudo Wire Type : Ethernet_VLAN
    Serial number for the session : 6
    Local Session ID : 129538998
    Remote Session ID : 8151374
    Size of local cookie (0, 4 or 8 bytes) : 0
    First word of local cookie : 0
    Second word of local cookie : 0
    Size of remote cookie (0, 4 or 8 bytes) : 0
    First word of remote cookie : 0
    Second word of remote cookie : 0
    Session state : Established
    Remote End ID : 444
    Trunk Session : 1
    Native VLAN tagged : Enabled
    Native VLAN ID : 0
    Number of packets received : 0
    Number of bytes received : 0
    Number of packets sent : 0
    Number of bytes sent : 0
    Number of packets dropped : 0
ap7131-11E6C4#
```

ldap-agent

show commands

Displays an LDAP agent's join status (join status to a LDAP server domain)

NOTE
This command is not available in the USER EXEC Mode.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show ldap-agent join-status {on <DEVICE-NAME>}
```

Parameters

```
show ldap-agent join-status {on <DEVICE-NAME>}
```

ldap-agent {on <DEVICE-NAME>}	Displays if a specified device (LDAP agent) has successfully joined a LDAP server's domain • on <DEVICE-NAME> – Optional. Specifies the device name. • <DEVICE-NAME> – Specify the name of the access point, wireless controller, or service platform.

Example

```
rfs6000-81701D#sh ldap-agent join-status
Primary LDAP Server's agent join-status : Joined domain SYMBOL.

Secondary LDAP Server's agent join-status : Not Configured
rfs6000-81701D#
```

licenses

show commands

Displays installed licenses and usage information

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show licenses {borrowed|lent}
```

Parameters

```
show licenses {borrowed|lent}
```

licenses {borrowed|lent}	Displays installed licenses and usage information • borrowed – Optional. Displays information on licenses borrowed • lent – Optional. Displays information on licenses lent

Usage Guidelines:

The Mobility HM network defines a three-tier structure, consisting of multiple wireless sites managed by a single *Network Operations Center* (NOC) controller, The NOC and the site controllers constitute the first and second tiers of the hierarchy respectively. The site controllers in turn adopt and manage access points that form the third tier of the hierarchy. The site controllers may or may not be grouped to form clusters.

At the time of adoption, access points and adaptive access points are provided license by the adopting controller. These license packs can be installed on both the NOC and site controllers. When a AP/AAP is adopted by a controller, the controller pushes a license on to the device. At this point the various possible scenarios are:

- AP/AAP license packs installed on the NOC controller only.

  The NOC controller provides the site controllers with the AP licenses, ensuring that per platform limits are not exceeded.

- AP/AAP license packs installed on the NOC and site controllers.

  The site controller uses its installed licenses and, in case of a shortage, the site controller borrows additional licenses from the NOC. If the NoC controller is unable to allocate sufficient licenses, the site controller unadopts some of the AP/AAPs.

- AP/AAP license packs installed on one controller within a cluster.

  The site controller shares its installed and borrowed licenses with other cluster controllers.

Example

```
rfs4000-229D58#show licenses
Serial Number : 9184521800027

Device Licenses:
  AP-LICENSE
    String     : DEFAULT-6AP-LICENSE
    Value      : 6
    Borrowed   : 0
    Total      : 6
    Used       : 0
  AAP-LICENSE
    String     :
    Value      : 0
    Borrowed   : 0
    Total      : 0
    Used       : 0
  ADVANCED-SECURITY
    String     : DEFAULT-ADV-SEC-LICENSE
rfs4000-229D58#

The following example shows the show > licenses command ouput on a NOC
controller:

nx4500-5CFA2B#show licenses
Serial Number : 6283529900127

Device Licenses:
  AP-LICENSE
    String     :
41a5a30ee9bb0bd78e943dba0a36ac34d3cdc66c956ef1f449d89f1c28beb032ac9747a8f0c9f
98f
    Value      : 1
  AAP-LICENSE
    String     :
41a5a30ee9bb0bd7f8d421c001f7c9cbd3cdc66c956ef1f41960aa2a030abb41ac9747a8f0c9f
98f
    Value      : 1

Total Licenses:
  AP-LICENSE
```

```
    Value      : 263
    Used       : 0
  AAP-LICENSE
    Value      : 329
    Used       : 3

Cluster Licenses:
  AP-LICENSE
    Value      : 257
    Used       : 0
  AAP-LICENSE
    Value      : 257
    Used       : 2


Active Members:
-------------------------------------------------------------------------------
-----------------------
        MEMBER             SERIAL        LIC TYPE   VALUE     LENT   TOTAL
NO.APS    NO.AAPS
-------------------------------------------------------------------------------
-----------------------
00-15-70-5C-FA-3B    6283529900127    AP         1       0      1       0
2
00-15-70-5C-FA-3B    6283529900127    AAP        1       0      1       -
-
-------------------------------------------------------------------------------
-----------------------

Non-Active Members:
-------------------------------------------------------------------------------
-----------------------
      MEMBER            SERIAL      LIC TYPE  VALUE   LENT   TOTAL
VALIDITY(HRS)
-------------------------------------------------------------------------------
-----------------------
00-15-70-81-70-1D    7295520400017    AP          1        1       0        93
days, 5 hours
00-15-70-81-70-1D    7295520400017    AAP         51       0       51       93
days, 5 hours
-------------------------------------------------------------------------------
-----------------------
nx4500-5CFA2B#
```

In the following example, the ‘VALIDITY(HRS)’ column specifies the validity period, in days and hours, of a lent license. On a NOC controller, a ‘VALIDITY(HRS)’ value of ‘current’ implies that the site controller is currently adopted. Whereas, a numerical ‘VALIDITY(HRS)’ value indicates the days and hours the lent license is valid for a site controller that is not reachable.

```
rfs7000-37FABE#show licenses lent
-------------------------------------------------------------------------------
---------------------------
MAC                 HOST-NAME         TYPE  LENT  BORROWER-MAC
BORROWER-HOST-NAME  VALIDITY(HRS)
-------------------------------------------------------------------------------
---------------------------
00-15-70-37-FA-BE   rfs7000-37FABE     AP    1     00-00-00-04-04-0A
rfs4000-04040A      93 days, 5 hours
```

```
 00-15-70-37-FA-BE  rfs7000-37FABE     AAP   1     00-00-00-04-04-0A
rfs4000-04040A      93 days, 5 hours
 00-15-70-37-FA-BE  rfs7000-37FABE     AAP   1     00-00-00-04-04-0B
rfs4000-04040B      93 days, 5 hours
 00-15-70-37-FA-BE  rfs7000-37FABE     AAP   1     00-00-00-04-04-0D
rfs4000-04040D      93 days, 5 hours
 00-15-70-37-FA-BE  rfs7000-37FABE     AAP   2     00-23-68-88-1E-4B
rfs4000-881E4B      current
 00-15-70-81-70-1D  rfs6000-81701D     AP    1     00-23-68-88-1E-4B
rfs4000-881E4B      current
--------------------------------------------------------------------------------
---------------------------
rfs7000-37FABE#

rfs4000-881E4B#show licenses borrowed
--------------------------------------------------------------------------------
MAC                HOST-NAME          TYPE      BORROWED  VALIDITY
--------------------------------------------------------------------------------
00-15-70-37-FD-89  rfs7000-37FD89    AAP      2        99 days, 23 hours
00-15-70-81-70-1D  rfs6000-81701D    AP       1        99 days, 23 hours
--------------------------------------------------------------------------------
rfs4000-881E4B#
```

lldp

show commands

Displays *Link Layer Discovery Protocol* (LLDP) information

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show lldp [neighbors|report]
show lldp neighbors {on <DEVICE-NAME>}
show lldp report {detail|on}
show lldp report {detail} {(on <DEVICE-OR-DOMAIN-NAME>)}
```

Parameters

```
show lldp neighbors {on <DEVICE-NAME>}
```

lldp	Displays an LLDP neighbors table or aggregated LLDP neighbors table
neighbors	Displays an LLDP neighbors table
on <DEVICE-NAME>	Optional. Displays an LLDP neighbors table on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
show lldp report {detail} {(on <DEVICE-OR-DOMAIN-NAME>)}
```

lldp	Displays an LLDP neighbors table or aggregated LLDP neighbors table
report detail	Displays an aggregated LLDP neighbors table • detail – Optional. Displays detailed aggregated LLDP neighbors table
on <DEVICE-NAME>	The following keyword is recursive and common to the 'report detail' parameter: • on <DEVICE-NAME> – Displays an aggregated LLDP neighbors table on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Example

```
rfs7000-37FABE(config)#show lldp neighbors
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show lldp neighbors on rfs7000-37FABE
rfs7000-37FABE(config)#
```

logging

show commands

Displays the network's activity log

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show logging {on <DEVICE-NAME>}
```

Parameters

```
show logging {on <DEVICE-NAME>}
```

logging {on <DEVICE-NAME>}	Displays logging information on a specified device • <DEVICE-NAME> – Optional. Specify the name of the AP, wireless controller, or service platform.

Example

```
rfs4000-229D58(config)#show logging on rfs4000-229D58

Logging module: enabled
    Aggregation time: disabled
    Console logging: level warnings
    Monitor logging: disabled
    Buffered logging: level warnings
    Syslog logging: level warnings
        Facility: local7

Log Buffer (359 bytes):
```

```
Jan 23 19:50:40 2013: rfs4000-229D58 : %SYSTEM-3-LOGIN_FAIL: Log-in failed for
user 'admin' from 'ssh'
Jan 22 00:04:14 2013: rfs4000-229D58 : %SYSTEM-3-UI_USER_AUTH_FAIL: UI user
'Admin' from: '192.168.13.10' authentication failed
Jan 21 23:56:32 2013: rfs4000-229D58 : %SYSTEM-3-UI_USER_AUTH_FAIL: UI user
'admin' from: '192.168.13.10' authentication failed
rfs4000-229D58(config)#
```

mac-access-list-stats

show commands

Displays MAC access list statistics

NOTE
This command is not present in USER EXEC mode.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show mac-access-list-stats {<MAC-ACCESS-LIST-NAME>|on}
show mac-access-list-stats {<MAC-ACCESS-LIST-NAME>} {(on <DEVICE-NAME>)}
```

Parameters

```
show mac-access-list-stats {<MAC-ACCESS-LIST-NAME>} {(on <DEVICE-NAME>)}
```

mac-access-list-stats	Displays MAC access list statistics
<MAC-ACCESS-LIST>	Optional. Displays statistics for a specified MAC access list. Specify the MAC access list name.
on <DEVICE-NAME>	Optional. Displays all or a specified MAC access list statistics on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Example

```
nx6524-5483B0#show mac-access-list stats scalemacacl | i 311
  permit D0-67-E5-3F-C0-00 FF-FF-FF-FF-F0-00  host 00-1E-EC-F2-0A-76
rule-precedence 311        Hitcount: 0        Hardware Hitcount: 0
nx6524-5483B0#
```

mac-address-table

show commands

Displays MAC address table entries

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show mac-address-table {on <DEVICE-NAME>}
```

Parameters

```
show mac-address-table {on <DEVICE-NAME>}
```

mac-address-table	Displays MAC address table entries
on <DEVICE-NAME>	Optional. Displays MAC address table entries on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Example

```
rfs7000-37FABE(config)#show mac-address-table on rfs7000-37FABE
------------------------------------------------------------
 BRIDGE VLAN PORT             MAC               STATE
------------------------------------------------------------
 1      1    ge1              00-02-B3-28-D1-55 forward
 1      1    ge1              00-23-68-11-E6-C4 forward
 1      1    ge1              00-A0-F8-68-D5-66 forward
 1      1    ge1              5C-D9-98-4C-04-51 forward
------------------------------------------------------------
Total number of MACs displayed: 4
rfs7000-37FABE(config)#
```

macauth

show commands

Displays details of wired ports that have MAC address authentication enabled

For more information on enabling MAC address authentication on a wired port, see *mac-auth*.

Supported in the following platforms:

- Access Points — Brocade Mobility 6511 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
show macauth [all|interface|on]

show macauth [all|interface [<INTERFACE-NAME>|ge <1-5>|port-channel
<1-3>|up1]]
          {(on <DEVICE-NAME>)}
```

Parameters

```
show macauth [all|interface [<INTERFACE-NAME>|ge <1-5>|port-channel
<1-3>|up1]]
{(on <DEVICE-NAME>)}
```

macauth	Displays MAC authentication related information for all interfaces or all interfaces
all	Displays MAC authentication related information for all interfaces
interface [<INTERFACE-NAME>| ge <1-5>| port-channel <1-3>|up1]	Displays MAC authentication related information for a specified interface. Specify the interface using one of the following options: • <INTERFACE-NAME> – Selects the interface identified by the <INTERFACE-NAME> keyword • ge <1-5> – Selects the GigabitEthernet interface identified by the index number • port-channel <1-3> – Selects the port channel interface identified by the index number • up1 – Selects the WAN Ethernet interface
on <DEVICE-NAME>	The following keywords are common to the 'all' and 'interface' parameters: • on <DEVICE-NAME> – Optional. Displays MAC authentication related information on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Example

```
rfs4000-229D58(config)#show macauth all
AAA-Policy is none

Mac Auth info for interface GE1
---------------------------------
 Mac Auth Enabled
 Mac Auth Not Authorized

Mac Auth info for interface GE2
---------------------------------
 Mac Auth Disabled
 Mac Auth Not Authorized

Mac Auth info for interface GE3
---------------------------------
 Mac Auth Disabled
 Mac Auth Not Authorized

Mac Auth info for interface GE4
---------------------------------
 Mac Auth Disabled
 Mac Auth Authorized

Mac Auth info for interface GE5
---------------------------------
 Mac Auth Disabled
 Mac Auth Not Authorized

Mac Auth info for interface UP1
---------------------------------
 Mac Auth Disabled
 Mac Auth Not Authorized
rfs4000-229D58(config)#
```

mint

show commands

Displays MiNT protocol configuration commands

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show mint
[config|dis|id|info|known-adopters|links|lsp|lsp-db|mlcp|neighbors|route|
          stats|tunnel-controller|tunneled-vlans]

show mint [config|id|info|known-adopters|route|stats|tunneled-vlans]
          {on <DEVICE-NAME>}

show mint [dis|links|neighbors|tunnel-controller] {details} {(on
<DEVICE-NAME>)}

show mint lsp

show mint lsp-db {details <MINT-ADDRESS>} {(on <DEVICE-NAME>)}

show mint mlcp {history} {(on <DEVICE-NAME>)}
```

Parameters

```
show mint [config|id|info|known-adopters|route|stats|tunneled-vlans] {on
<DEVICE-NAME>}
```

mint	Displays MiNT protocol information based on the parameters passed
config	Displays MiNT configuration
id	Displays local MiNT ID
info	Displays MiNT status
known-adopters	Displays known, possible, or reachable adopters
route	Displays MiNT route table details
stats	Displays MiNT related statistics
tunneled-vlans	Displays MiNT tunneled VLAN details
on <DEVICE-NAME>	The following keywords are common to all of the above parameters: • on <DEVICE-NAME> – Optional. Displays MiNT protocol details on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
show mint [dis|links|neighbors|tunnel-controller] {details} {(on
<DEVICE-NAME>)}
```

mint	Displays MiNT protocol information based on the parameters passed
dis	Displays MiNT network *Designated Intermediate Systems* (DISes) and EVISes
links	Displays MiNT networking link details
neighbors	Displays adjacent MiNT peer details

tunnel-controller	Displays details of MiNT VLAN network tunnel wireless controllers for extended VLAN load balancing
details {(on <DEVICE-NAME>)}	The following keywords are common to the 'dis', 'links', 'neighbors', and 'tunnel-controller' parameters: • details – Optional. Displays detailed MiNT information • on <DEVICE-NAME> – Optional. This is a recursive parameter, which displays MiNT information on a specified device

`show mint lsp`

mint	Displays MiNT protocol information based on the parameters passed
lsp	Displays this router's MiNT *Label Switched Paths* (LSPs)

`show mint lsp-db {details <MINT-ADDRESS>} {(on <DEVICE-NAME>)}`

mint	Displays MiNT protocol information based on the parameters passed
lsp-db	Displays MiNT LSP database entries
details <MINT_ADDRESS>	Optional. Displays detailed MiNT LSP database entries • <MINT_ADDRESS> – Specify the MiNT address in the AA.BB.CC.DD format.
on <DEVICE-NAME>	The following keyword is recursive and common to the 'details' parameter: • on <DEVICE-NAME> – Optional. Displays MiNT LSP database entries on a specified device • <DEVICE-NAME> – Specify the name of the AP or wireless controller

`show mint mlcp {history} {(on <DEVICE-NAME>)}`

mint	Displays MiNT protocol information based on the parameters passed
mlcp	Displays *MiNT Link Creation Protocol* (MLCP) status
history	Optional. Displays MLCP client history • on <DEVICE-NAME> – Optional. Displays MLCP client history on a specified device
on <DEVICE-NAME>	The following keyword is recursive and common to the 'history' parameter: • on <DEVICE-NAME> – Optional. Displays MLCP client history on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Example

```
rfs7000-37FABE(config)#show mint stats
0 L1 neighbors
L1 LSP DB size 1 LSPs (0 KB)
1 L1 routes
Last SPFs took 0s
SPF (re)calculated 1 times.
levels 1
base priority 180
dis priority 180
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show mint lsp
id 70.37.fa.be, level 1, seqnum 18640, 0 adjacencies, 0 extended-vlans,
expires in 1145 seconds, republish in 722 seconds, changed True,
ext-vlan FDB pri 0, 180 bytes

rfs7000-37FABE(config)#show mint lsp-db
1 LSPs in LSP-db of 70.37.FA.BE:
LSP 70.37.FA.BE at level 1, hostname "rfs7000-37FABE", 0 adjacencies, seqnum
84941
rfs7000-37FABE(config)#
```

```
rfs7000-37FABE(config)#show mint route on rfs7000-37FABE
Destination : Next-Hop(s)
70.37.FA.BE : 70.37.FA.BE via self
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show mint known-adopters on rfs7000-37FABE
70.37.FA.BE
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show mint config
Base priority 180
DIS priority 180
Control priority 180
UDP/IP Mint encapsulation port 24576
Global Mint MTU 1500
rfs7000-37FABE(config)#
```

ntp

show commands

Displays *Network Time Protocol* (NTP) information. NTP enables clock synchronization within a network.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show ntp [associations|status]
show ntp [associations {detail|on}|status {on <DEVICE-NAME>}]
```

Parameters

```
show ntp [associations {detail|on}|status {on <DEVICE-NAME>}]
```

ntp associations {detail|on}	Displays existing NTP associations • detail – Optional. Displays detailed NTP associations • on <DEVICE-NAME> – Optional. Displays NTP associations on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.
ntp status {on <DEVICE-NAME>}	Displays NTP association status • on <DEVICE-NAME> – Optional. Displays NTP association status on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Example

```
rfs7000-37FABE>show ntp associations
 address     ref clock    st when poll reach delay offset  disp
 * master (synced), # master (unsynced), + selected, - candidate, ~ configured
rfs7000-37FABE>
```

```
rfs7000-37FABE>show ntp status
Clock is synchronized, stratum 0, actual frequency is 0.0000 Hz, precision is
2**0
reference time is 00000000.00000000 (Feb 07 06:28:16 UTC 2036)
clock offset is 0.000 msec, root delay is 0.000 msec
root dispersion is 0.000 msec
rfs7000-37FABE>
```

password-encryption

show commands

Displays password encryption status (enabled/disabled)

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show password-encryption status
```

Parameters

```
show password-encryption status
```

password-encryption status	Displays password encryption status (enabled/disabled)

Example

```
rfs7000-37FABE(config)#show password-encryption status
Password encryption is disabled
rfs7000-37FABE(config)#
```

pppoe-client

show commands

Displays *Point-to-Point Protocol over Ethernet* (PPPoE) client information

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show pppoe-client [configuration|status] {on <DEVICE-NAME>}
```

Parameters

```
show pppoe-client [configuration|status] {on <DEVICE-NAME>}
```

pppoe-client	Displays PPPoE client information (configuration and status)
configuration	Displays detailed PPPoE client configuration
status	Displays detailed PPPoE client status
on <DEVICE-NAME>	The following keywords are common to 'configuration' and 'status' parameters: • on <DEVICE-NAME> – Optional. Displays detailed PPPoE client status or configuration on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Example

```
rfs7000-37FABE(config)#show pppoe-client configuration
 PPPoE Client Configuration:
+----------------------------------------
|  Mode          : Disabled
|  Service Name  :
|  Auth Type     : pap
|  Username      :
|  Password      :
|  Idle Time     : 600
|  Keepalive     : Disabled
|  Local n/w     : vlan1
|  Static IP     : 0.0.0.0
|  MTU           : 1492
+----------------------------------------

rfs7000-37FABE(config)#
```

privilege

show commands

Displays a device's existing privilege level

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show privilege
```

Parameters

None

Example

```
rfs7000-37FABE(config)#show privilege
Current user privilege: superuser
```

```
rfs7000-37FABE(config)#
```

reload

show commands

Displays scheduled reload information for a specific device

NOTE
This command is not present in the USER EXEC mode.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show reload {on <DEVICE-OR-DOMAIN-NAME>}
```

Parameters

```
show reload {on <DEVICE-OR-DOMAIN-NAME>}
```

reload {on <DEVICE-OR-DOMAIN-NAME>}	Displays scheduled reload information for a specified device • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays configuration on a specified device • <DEVICE-OR_DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

Example

```
rfs7000-37FABE(config)#show reload on rfs7000-37FABE
No reload is scheduled.
rfs7000-37FABE(config)#
```

rf-domain-manager

show commands

Displays RF Domain manager selection details

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show rf-domain-manager {on <DEVICE-OR-DOMAIN-NAME>}
```

Parameters

```
show rf-domain-manager {on <DEVICE-OR-DOMAIN-NAME>}
```

rf-domain-manager	Displays RF Domain manager selection details
on <DEVICE-OR-DOMAIN-NAME>	Optional. Displays RF Domain manager selection details on a specified device or domain • <DEVICE-OR-DOMAIN-NAME> – specify the name of the AP, wireless controller, service platform, or RF Domain.

Example

```
rfs7000-37FABE(config)#show rf-domain-manager on rfs7000-37FABE
 RF Domain RFDOMAIN_TechPubsLabLan
 RF Domain Manager:
    ID: 70.37.FA.BE
    Priority: 180
    Has IP MiNT link
    Has wired MiNT links
 Device under query:
    Priority: 180
    Has IP MiNT links
    Has wired MiNT links
rfs7000-37FABE(config)#
```

role

show commands

Displays role based firewall information

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show role [ldap-stats|wireless-clients]
show role [ldap-stats|wireless-clients] {on <DEVICE-NAME>}
```

Parameters

```
show role [ldap-stats|wireless-clients] {on <DEVICE-NAME>}
```

role ldap-stats	Displays LDAP server status and statistics • on <DEVICE-NAME> – Optional. Displays LDAP server status on a specified device
role wireless-clients	Displays clients associated with roles • on <DEVICE-NAME> – Optional. Displays clients associated with roles on a specified device

Example

```
rfs7000-37FABE(config)#show role wireless-clients on rfs7000-37FABE
```

```
No ROLE statistics found.
rfs7000-37FABE(config)#
```

route-maps

show commands

Displays route map statistics for defined device routes

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show route-maps {on <DEVICE-NAME>}
```

Parameters

```
show route-maps {on <DEVICE-NAME>}
```

route-maps	Displays configured route map statistics for all defined routes **NOTE:** For more information on route maps, see *route-map on page 25-1243*.
on <DEVICE-NAME>	Optional. Displays route map statistics on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Example

```
rfs7000-37FABE(config)#show route-maps on rfs7000-37FABE
rfs7000-37FABE(config)#
```

rtls

show commands

Displays *Real Time Location Service* (RTLS) statistics for access points contributing locationing information

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show rtls [aeroscout|ekahau] {<MAC/HOSTNAME>} {(on <DEVICE-OR-DOMAIN-NAME>)}
```

Parameters

`show rtls [aeroscout|ekahau] {<MAC/HOSTNAME>} {(on <DEVICE-OR-DOMAIN-NAME>)}`

rtls	Displays access point RTLS statistics
aeroscout	Displays access point Aeroscout statistics
ekahau	Displays access point Ekahau statistics
<MAC/HOSTNAME>	Optional. Displays Aeroscout or Ekahau statistics for a specified access point. Specify the MAC address or hostname of the access point.
on <DEVICE-OR-DOMAIN-NAME>	The following keyword is recursive and common to 'Aeroscout' and 'Ekahau' parameters: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays Aeroscout or Ekahau statistics on a specified device or domain. • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

Example

```
rfs4000-229D58(config)#show rtls aeroscout

 Aeroscout Engine IP: 0.0.0.0 Port: 0
 Send Count           : 0
 Recv Count           : 0
 Tag Reports          : 0
 Nacks                : 0
 Acks                 : 0
 Lbs                  : 0
 AP Status            : 0
 AP Notif             : 0
 Send Err             : 0
 Errmsg Count         : 0

Total number of APs displayed: 1
rfs4000-229D58(config)#
```

running-config

show commands

Displays configuration files (where all configured MAC and IP access lists are applied to an interface)

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show running-config
{aaa-policy|association-acl-policy|auto-provisioning-policy|

captive-portal-policy|device|dhcp-server-policy|firewall-policy|include-facto
```

```
ry|

interface|ip-access-list|mac-access-list|management-policy|meshpoint|profile|
          radio-qos-policy|rf-domain|smart-rf-policy|wlan|wlan-qos-policy}

show running-config
{aaa-policy|association-acl-policy|auto-provisioning-policy|

captive-portal-policy|dhcp-server-policy|firewall-policy|management-policy|
          radio-qos-policy|smart-rf-policy|wlan-qos-policy} <POLICY-NAME>
{include-factory}

show running-config {device [<MAC>|self]} {include-factory}

show running-config {include-factory}

show running-config {interface}
{<INTERFACE-NAME>|ge|include-factory|me|port-channel|
          pppoe1|vlan|wwan1}
show running-config {interface} {<INTERFACE-NAME>|ge <1-4>|include-factory|
          me1|port-channel <1-2>|pppoe1|vlan <1-4094>|wwan1}
{include-factory}

show running-config {ip-access-list <IP-ACCESS-LIST-NAME>|mac-access-list
<MAC-ACCESS-
          LIST-NAME} {include-factory}

show running-config {meshpoint <MESHPOINT-NAME>} {include-factory}

show running-config {profile
[|ap622|br650|br6511|ap6521|br1220|ap6532|ap6562|
          br71xx|br81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx9000]
<PROFILE-NAME>}
          {include-factory}

show running-config {rf-domain <DOMAIN-NAME>} {include-factory}

show running-config {wlan <WLAN-NAME>} {include-factory}
```

Parameters

```
show running-config
{aaa-policy|association-acl-policy|auto-provisioning-policy|
captive-portal-policy|dhcp-server-policy|firewall-policy|management-policy|
radio-qos-policy|smart-rf-policy|wlan-qos-policy} <POLICY-NAME>
{include-factory}
```

running-config	Optional. Displays current running configuration
aaa-policy	Optional. Displays AAA policy configuration
association-acl-policy	Optional. Displays association ACL policy configuration
auto-provisioning-policy	Optional. Displays auto provisioning policy configuration
captive-portal-policy	Optional. Displays captive portal policy configuration
dhcp-server-policy	Optional. Displays the DHCP server policy configuration
firewall-policy	Optional. Displays firewall policy configuration
management-policy	Optional. Displays management policy configuration
radio-qos-policy	Optional. Displays radio QoS policy configuration

smart-rf-policy	Optional. Displays Smart RF policy configuration
wlan-qos-policy	Optional. Displays WLAN QoS policy configuration
<POLICY-NAME>	The following keyword is common to all policies: • <POLICY-NAME> – Specify the name of the policy.
include-factory	The following keyword is common to all policies: • include-factory – Optional. Includes factory defaults

`show running-config {device [<MAC>|self]} {include-factory}`

running-config	Displays current running configuration
device [<MAC>|self]	Optional. Displays device configuration • <MAC> – Displays a specified device configuration. Specify the MAC address of the device. • self – Displays the logged device's configuration
include-factory	The following keyword is common to the '<MAC>' and 'self' parameters: • Optional. Displays factory defaults

`show running-config {include-factory}`

running-config	Displays current running configuration
include-factory	Optional. Includes factory defaults

`show running-config {interface} {<INTERFACE-NAME>|ge <1-4>|include-factory|me1|port-channel <1-2>|pppoe1|vlan <1-4094>|wwan1} {include-factory}`

running-config	Displays current running configuration
interface	Optional. Displays interface configuration
<INTERFACE-NAME>	Optional. Displays a specified interface configuration. Specify the interface name.
ge <1-4>	Optional. Displays GigabitEthernet interface configuration • <1-4> – Specify the GigabitEthernet interface index from 1 - 4.
me1	Optional. Displays FastEthernet interface configuration
port-channel <1-2>	Optional. Displays port channel interface configuration • <1-2> – Specify the port channel interface index from 1 - 2.
pppoe1	Optional. Displays PPP over Ethernet interface configuration
vlan <1-4094>	Displays VLAN interface configuration • <1-4094> – Specify the VLAN interface number from 1 - 4094.
wwan1	Optional. Displays Wireless WAN interface configuration
include-factory	The following keyword is common to all interfaces: • Optional. Includes factory defaults

`show running-config {ip-access-list <IP-ACCESS-LIST-NAME>|mac-access-list <MAC-ACCESS-LIST-NAME} {include-factory}`

running-config	Displays current running configuration
ip-access-list <IP-ACCESS-LIST-NAME>	Optional. Displays IP access list configuration • <IP-ACCESS-LIST-NAME> – Specify the IP access list name
mac-access-list <MAC-ACCESS-LIST-NAME>	Optional. Displays MAC access list configuration • <MAC-ACCESS-LIST-NAME> – Specify the MAC access list name
include-factory	The following keyword is common to the 'ip-access-list' and 'mac-access-list' parameters: • Optional. Includes factory defaults

show running-config *{meshpoint <MESHPOINT-NAME>} {include-factory}*	
running-config	Displays current running configuration
meshpoint <MESHPOINT-NAME>	Optional. Displays meshpoint configuration • <MESHPOINT-NAME> – Specify the meshpoint name
include-factory	Optional. Includes factory defaults along with running configuration details

show running-config *{profile [br650|br6511|br1220|br71xx|br81xx|rfs4000|rfs6000|rfs7000] <PROFILE-NAME>} {include-factory}*	
running-config	Displays current running configuration
profile	Optional. Displays current configuration for a specified profile
br650 <PROFILE-NAME>	Displays Brocade Mobility 650 Access Point profile configuration • <PROFILE-NAME> – Displays configuration for a specified Brocade Mobility 650 Access Point profile. Specify the Brocade Mobility 650 Access Point profile name.
br6511 <PROFILE-NAME>	Displays Brocade Mobility 6511 Access Point profile • <PROFILE-NAME> – Displays configuration for a specified Brocade Mobility 6511 Access Point profile. Specify the Brocade Mobility 6511 Access Point profile name.
br1220 <PROFILE-NAME>	Displays Brocade Mobility 1220 Access Point profile configuration • <PROFILE-NAME> – Displays configuration for a specified Brocade Mobility 1220 Access Point profile. Specify the Brocade Mobility 1220 Access Point profile name.
br71xx <PROFILE-NAME>	Displays Brocade Mobility 71XX Access Point profile configuration • <PROFILE-NAME> – Displays configuration for a specified Brocade Mobility 71XX Access Point profile. Specify the Brocade Mobility 71XX Access Point profile name.
br81xx <PROFILE-NAME>	Displays Brocade Mobility 1240 Access Point profile configuration • <PROFILE-NAME> – Displays configuration for a specified Brocade Mobility 1240 Access Point profile. Specify the Brocade Mobility 1240 Access Point profile name.
rfs4000 <PROFILE-NAME>	Displays Brocade Mobility RFS4000 profile configuration • <PROFILE-NAME> – Displays configuration for a specified Brocade Mobility RFS4000 profile. Specify the Brocade Mobility RFS4000 profile name.
rfs6000 <PROFILE-NAME>	Displays Brocade Mobility RFS6000 profile configuration • <PROFILE-NAME> – Displays configuration for a specified Brocade Mobility RFS6000 profile. Specify the Brocade Mobility RFS6000 profile name.
rfs7000 <PROFILE-NAME>	Displays Brocade Mobility RFS7000 profile configuration • <PROFILE-NAME> – Displays configuration for a specified Brocade Mobility RFS7000 profile. Specify the Brocade Mobility RFS7000 profile name.
include-factory	Optional. This parameter is common to all profiles. It includes factory defaults

show running-config *{rf-domain <DOMAIN-NAME>} {include-factory}*	
running-config	Displays current running configuration
rf-domain <DOMAIN-NAME>	Optional. Displays current configuration for a RF Domain • <DOMAIN-NAME> – Displays current configuration for a specified RF Domain. Specify the RF Domain name.
include-factory	Optional. Includes factory defaults

```
show running-config {wlan <WLAN-NAME>} {include-factory}
```

running-config	Displays current running configuration
wlan <WLAN-NAME>	Optional. Displays current configuration for a WLAN • <WLAN-NAME> – Displays current configuration for a specified WLAN. Specify the WLAN name.
include-factory	Optional. Includes factory defaults

Example

```
rfs7000-37FABE(config)#show running-config device self
!
firewall ratelimit-trust policy default
!
management-policy default
 telnet
 http server
 ssh
!
firewall-policy default
!
mint-security-policy the_policy
 rejoin-timeout 35
!
device-discover-policy default
!
rfs7000 00-15-70-37-FA-BE
 hostname rfs7000-37FABE
 no country-code
 bridge vlan 3
 bridge vlan 5
  ip dhcp trust
  ip igmp snooping querier version 2
  ip igmp snooping querier max-response-time 3
  ip igmp snooping querier timer expiry 89
 wep-shared-key-auth
 radius nas-identifier test
--More--
rfs7000-37FABE(config)

rfs7000-37FABE(config)#show running-config device 11-22-33-44-55-66
include-factory
!
radio-qos-policy default
 wmm best-effort aifsn 3
 wmm video txop-limit 94
 wmm video aifsn 1
 wmm video cw-min 3
 wmm video cw-max 4
 wmm voice txop-limit 47
 wmm voice aifsn 1
 wmm voice cw-min 2
--More--
rfs7000-37FABE(config)

nx6500-31FABE(config)#show running-config device 11-22-33-44-55-66
include-factory
!
radio-qos-policy default
 wmm best-effort aifsn 3
```

```
 wmm video txop-limit 94
 wmm video aifsn 1
 wmm video cw-min 3
 wmm video cw-max 4
 wmm voice txop-limit 47
 wmm voice aifsn 1
 wmm voice cw-min 2
--More--
nx6500-31FABE(config)#
```

session-changes

show commands

Displays configuration changes made in the current session

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show session-changes
```

Parameters

None

Example

```
rfs7000-37FABE(config)#show session-changes

No changes in this session

rfs7000-37FABE(config)#
```

session-config

show commands

Lists active open sessions on a device

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show session-config {include-factory}
```

Parameters

```
show session-config {include-factory}
```

session-config include-factory	Displays current session configuration • include-factory – Optional. Includes factory defaults

Example

```
rfs4000-229D58(config)#show session-config
!
! Configuration of Brocade Mobility RFS4000 version 5.5.0.0-036B
!
!
version 2.3
!
!
client-identity TestClientIdentity
 dhcp 1 message-type request option-codes exact hexstring 5e4d36780b3a7f
!
client-identity-group ClientIdentityGroup
 client-identity TestClientIdentity precedence 1
!
alias network testNetworkAlias address-range 192.168.13.4 to 192.168.13.10
!
ip access-list BROADCAST-MULTICAST-CONTROL
 permit tcp any any rule-precedence 10 rule-description "permit all TCP
traffic"
 permit udp any eq 67 any eq dhcpc rule-precedence 11 rule-description "permit
DHCP replies"
 deny udp any range 137 138 any range 137 138 rule-precedence 20
rule-description "deny windows netbios"
 deny ip any 224.0.0.0/4 rule-precedence 21 rule-description "deny IP
multicast"
 deny ip any host 255.255.255.255 rule-precedence 22 rule-description "deny IP
l
--More--
rfs4000-229D58(config)#
```

sessions

show commands

Displays CLI sessions initiated on a device

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show sessions {on <DEVICE-NAME>}
```

Parameters

```
show sessions {on <DEVICE-NAME>}
```

sessions	Displays CLI sessions initiated on a device
on <DEVICE-NAME>	Optional. Displays CLI sessions on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Example

```
rfs4000-229D58(config)#show sessions
INDEX   COOKIE  NAME           START TIME             FROM                 ROLE
1       49      admin           2013-02-15 15:45:10     192.168.100.225
superuser
2       2       snmp            2013-01-16 22:37:59     127.0.0.1
superuser
3       3       snmp2           2013-01-16 22:37:59     127.0.0.1
superuser

rfs4000-229D58(config)#
```

site-config-diff

show commands

Displays the difference in site configuration available on the NOC and a site.

The Mobility HM network defines a three-tier structure, consisting of multiple wireless sites managed by a single *Network Operations Center* (NOC) controller, The NOC controller constitutes the first and the site controllers constitute the second tier of the hierarchy. The site controllers may or may not be grouped to form clusters. The site controllers in turn adopt and manage access points that form the third tier of the hierarchy.

NOC controllers possess default site configuration details. Overrides applied at the site level result in a mismatch of configuration at the site and the default site configuration available on the NOC controller. Use this command to view this difference.

Supported in the following platforms:

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

NOTE
This command returns an output only when executed on a NOC controller.

Syntax:

```
show site-config-diff <SITE-NAME>
```

Parameters

```
show site-config-diff <SITE-NAME>
```

site-config-diff <SITE-NAME>	Displays the configuration difference for the specified site • <SITE-NAME> – Specify the site name.

Example

```
nx9500-6C874D#show site-config-diff 5C-0E-8B-18-06-F4
---- Config diff for switch 5C-0E-8B-18-06-F4 ----
rfs6000 5C-0E-8B-18-06-F4
interface pppoe1
  no shutdown
nx9500-6C874D#
```

smart-rf

show commands

Displays Smart RF management commands

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show smart-rf [br|calibration-config|calibration-status|channel-distribution|

history|history-timeline|interfering-br|interfering-neighbors|radio]

show smart-rf br {<MAC>|<DEVICE-NAME>|activity|energy|neighbors|on
<DOMAIN-NAME>}
show smart-rf br {<MAC>|<DEVICE-NAME>} {on <DOMAIN-NAME>}
show smart-rf br (activity|energy|neighbors} [<MAC>|<DEVICE-NAME>] {(on
<DOMAIN-NAME>)}

show smart-rf [calibration-config|calibration-status|channel-distribution|
          history|history-timeline] {on <DOMAIN-NAME>}

show smart-rf radio
{<MAC>|activity|all-11an|all-11bgn|channel|energy|neighbors|
          on <DOMAIN-NAME>}
show smart-rf radio {<MAC>|all-11an|all-11bgn|energy <MAC>} {on <DOMAIN-NAME>}
show smart-rf radio {activity|neigbors} {<MAC>|all-11an|all-11bgn} {on
<DOMAIN-NAME>}

show smart-rf interfering-br {<MAC>|<DEVICE-NAME>|on}

show smart-rf interfering-neighbors {<MAC>|<DEVICE-NAME>|on|threshold
<50-100>}
```

Parameters

```
show smart-rf br {<MAC>|<DEVICE-NAME>} {on <DOMAIN-NAME>}
```

br	Displays access point related commands
<MAC>	Optional. Uses MAC addresses to identify access points. Displays all access points, if no MAC address is specified.

<DEVICE-NAME>	Optional. Uses an administrator defined name to identify an access point
on <DOMAIN-NAME>	Optional. Displays access point details on a specified RF Domain. Specify the domain name.

`show smart-rf br (activity|energy|neighbors} [<MAC>|<DEVICE-NAME>] {(on <DOMAIN-NAME>)}`

br	Displays AP related commands
activity	Optional. Displays AP activity for a specified AP or all APs
energy	Optional. Displays AP energy for a specified AP or all APs
neighbors	Optional. Displays AP neighbors
{<MAC>| <DEVICE-NAME>}	The following keywords are common to all of the above parameters: • <MAC> – Displays a specified AP related information. Uses MAC address to identify the AP • <DEVICE-NAME> – Displays a specified AP related information. Uses device name to identify the AP
on <DOMAIN-NAME>	Optional.Displays access point details on a specified RF Domain. Specify the domain name.

`show smart-rf [calibration-config|calibration-status|channel-distribution|history|history-timeline] {on <DOMAIN-NAME>}`

calibration-config	Displays interactive calibration configurations
calibration-status	Displays Smart RF calibration status
channel-distribution	Displays Smart RF channel distribution
history	Displays Smart RF calibration history
history-timeline	Displays extended Smart RF calibration history on an hourly or daily timeline
on <DOMAIN-NAME>	This parameter is common to all of above smart RF options: • on <DOMAIN-NAME> – Optional. Displays Smart RF configuration, based on the parameters passed, on a specified RF Domain • on <DOMAIN-NAME> – Specify the RF Domain name.

`show smart-rf radio {<MAC>|all-11an|all-11bgn|energy <MAC>} {on <DOMAIN-NAME>}`

radio	Displays radio related commands
<MAC>	Optional. Displays details of a specified radio. Specify the radio's MAC address in the AA-BB-CC-DD-EE-FF format.
all-11an	Optional. Displays all 11a radios currently in the configuration
all-11bgn	Optional. Displays all 11bg radios currently in the configuration
energy {<MAC>}	Optional. Displays radio energy Specify the MAC address of the radio • <MAC> – Optional. Specify the radio's MAC address in the AA-BB-CC-DD-EE-FF format.
on <DOMAIN-NAME>	The following keyword is common to above parameters: • on <DOMAIN-NAME> – Optional. Displays radio details on a specified RF Domain • <DOMAIN-NAME> – Specify the RF Domain name.

`show smart-rf radio {activity|neighbors} {<MAC>|all-11an|all-11bgn} {on <DOMAIN-NAME>}`

radio	Displays radio related commands
activity	Optional. Displays changes related to radio power, number of radio channels, or coverage holes. Use additional filters to view specific details.

<MAC>	Optional. Displays radio activity for a specified radio • <MAC> – Specify the radio's MAC address.
all-11an	Optional. Displays radio activity of all 11a radios in the configuration
all-11bgn	Optional. Displays radio activity of all 11bg radios in the configuration
on <DOMAIN-NAME>	Optional. Displays radio activity of all radios within a specified RF Domain • <DOMAIN-NAME> – Specify the RF Domain name.

`show smart-rf interfering-br {<MAC>|<DEVICE-NAME>|on}`

interfering-br	Displays interfering access points (requiring potential isolation) information
<MAC>	Optional. Displays information of a specified interfering access point • <MAC> – Specify the access point's MAC address. **NOTE:** Considers all APs if this parameter is omitted
<DEVICE-NAME>	Optional. Displays interfering access point information on a specified device • <DEVICE-NAME> – Specify the device name. **NOTE:** Considers all APs if this parameter is omitted
on <DOMAIN-NAME>	Optional. Displays all interfering access point information within a specified RF Domain • <DOMAIN-NAME> – Specify the RF Domain name.

`show smart-rf interfering-neighbors {<MAC>|<DEVICE-NAME>|on|threshold <50-100>}`

interfering-br	Displays interfering neighboring access point information
<MAC>	Optional. Displays interfering neighboring access point information • <MAC> – Specify the access point's MAC address. **NOTE:** Considers all APs if this parameter is omitted
<DEVICE-NAME>	Optional. Displays all interfering neighboring access point information on a specified device • <DEVICE-NAME> – Specify the device name. **NOTE:** Considers all APs if this parameter is omitted
threshold <50-100>	Specifies the maximum attenuation threshold of interfering neighbors. Specify a value from 50 -100.
on <DOMAIN-NAME>	Optional. Displays radio activity of all radios within a specified RF Domain • <DOMAIN-NAME> – Specify the RF Domain name.

Example

```
rfs7000-37FABE(config)#show smart-rf calibration-status
No calibration currently in progress
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show smart-rf history
----------------------------------------------------------------------------------
----------
      TIME                    EVENT                      DESCRIPTION
----------------------------------------------------------------------------------
----------
----------------------------------------------------------------------------------
----------
Total number of history entries displayed: 0
rfs7000-37FABE(config)#
```

spanning-tree

show commands

Displays spanning tree utilization information

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show spanning-tree mst {configuration|detail|instance|on}

show spanning-tree mst {configuration} {(on <DEVICE-NAME>)}

show spanning-tree mst {detail} {interface|on}
show spanning-tree mst {detail} interface {<INTERFACE-NAME>|ge <1-4>|me1|
          port-channel <1-2>|pppoe1|vlan <1-4094>|wwan1} {(on <DEVICE-NAME>)}

show spanning-tree mst {instance <1-15>} {interface <INTERFACE-NAME>}
          {(on <DEVICE-NAME>)}
```

Parameters

```
show spanning-tree mst {configuration} {(on <DEVICE-NAME>)}
```

spanning-tree	Displays spanning tree utilization information
mst	Displays *Multiple Spanning Tree* (MST) related information
configuration {on <DEVICE-NAME>}	Optional. Displays MST configuration • on <DEVICE-NAME> – Optional. Displays MST configuration on a specified device • <DEVICE-NAME> – Specify the name of the AP or wireless controller.

```
show spanning-tree mst {detail} interface {<INTERFACE-NAME>|ge <1-4>|me1|
port-channel <1-2>|pppoe1|vlan <1-4094>|wwan1} {(on <DEVICE-NAME>)}
```

spanning-tree	Displays spanning tree information
mst	Displays MST configuration
detail	Optional. Displays detailed MST configuration, based on the parameters passed

interface [<INTERFACE>| age <1-4>|me1| port-channel <1-2>| pppoe1| van <1-4094> wwan1]	Displays detailed MST configuration for a specified interface • <INTERFACE> – Displays detailed MST configuration for a specified interface. Specify the interface name. • age <1-4> – Displays GigabitEthernet interface MST configuration • <1-4> – Select the GigabitEthernet interface index from 1 - 4. • pppoe1 – Displays PPP over Ethernet interface MST configuration • vlan – Displays VLAN interface MST configuration • <1-4094> – Select the SVI VLAN ID from 1 - 4094. • wwan1 – Displays Wireless WAN interface MST configuration
on <DEVICE-NAME>	The following keyword is common to all interfaces: Optional. Displays detailed MST configuration on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
show spanning-tree mst {instance <1-15>} {interface <INTERFACE-NAME>}
{(on <DEVICE-NAME>)}
```

spanning-tree	Displays spanning tree information
mst	Displays MST configuration. Use additional filters to view specific details.
instance <1-15>	Optional. Displays information for a particular MST instance • <1-15> – Specify the instance ID from 1 - 15.
interface <INTERFACE-NAME>	Optional. Displays MST configuration for a specific interface instance. The options are: • <INTERFACE-NAME> – Displays MST configuration for a specified interface. Specify the interface name.
on <DEVICE-NAME>	Optional. Displays MST configuration on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Example

```
rfs7000-37FABE(config)#show spanning-tree mst configuration on rfs7000-37FABE
%%
%  MSTP Configuration Information for bridge 1 :
%%--------------------------------------------------------
%  Format Id      : 0
%  Name           : My Name
%  Revision Level : 0
%  Digest         : 0xac36177f50283cd4b83821d8ab26de62
%%--------------------------------------------------------

rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show spanning-tree mst detail interface test on
rfs7000-37FABE
% Bridge up - Spanning Tree Disabled
% CIST Root Path Cost 0  - CIST Root Port 0 - CIST Bridge Priority 32768
% Forward Delay 15 - Hello Time 2 - Max Age 20 - Max hops 20
% 1: CIST Root Id 800000157037fabf
% 1: CIST Reg Root Id 800000157037fabf
% 1: CIST Bridge Id 800000157037fabf
% portfast bpdu-filter disabled
% portfast bpdu-guard disabled
% portfast portfast errdisable timeout disabled
% portfast errdisable timeout interval 300 sec
% cisco interoperability not configured - Current cisco interoperability off

rfs7000-37FABE(config)#
```

```
rfs7000-37FABE(config)#show spanning-tree mst detail
% Bridge up - Spanning Tree Disabled
% CIST Root Path Cost 0  - CIST Root Port 0 - CIST Bridge Priority 32768
% Forward Delay 15 - Hello Time 2 - Max Age 20 - Max hops 20
% 1: CIST Root Id 800000157037fabf
% 1: CIST Reg Root Id 800000157037fabf
% 1: CIST Bridge Id 800000157037fabf
% portfast bpdu-filter disabled
% portfast bpdu-guard disabled
% portfast portfast errdisable timeout disabled
% portfast errdisable timeout interval 300 sec
% cisco interoperability not configured - Current cisco interoperability off

%   ge4: Port 2004 - Id 87d4 - Role Disabled - State Forwarding
%   ge4: Designated External Path Cost 0 - Internal Path Cost 0
%   ge4: Configured  Path Cost 11520 - Add type Implicit - ref count 1
%   ge4: Designated Port Id 0 - CST Priority 128
%   ge4: ge4: CIST Root 0000000000000000
%   ge4: ge4: Regional Root 0000000000000000
%   ge4: ge4: Designated Bridge 0000000000000000
%   ge4: Message Age 0 - Max Age 0
%   ge4: CIST Hello Time 0 - Forward Delay 0
%   ge4: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%   ge4: Version Multiple Spanning Tree Protocol - Received None - Send MSTP
--More--
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show spanning-tree mst instance 1 interface test on
rfs7000-37FABE
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show spanning-tree mst detail
% Bridge up - Spanning Tree Disabled
% CIST Root Path Cost 0  - CIST Root Port 0 - CIST Bridge Priority 32768
% Forward Delay 15 - Hello Time 2 - Max Age 20 - Max hops 20
% 1: CIST Root Id 800000157037fabf
% 1: CIST Reg Root Id 800000157037fabf
% 1: CIST Bridge Id 800000157037fabf
% 1: portfast bpdu-guard disabled
% portfast portfast errdisable timeout disabled
% portfast errdisable timeout interval 300 sec
% cisco interoperability not configured - Current cisco interoperability off
%   --More--
```

startup-config

show commands

Displays complete startup configuration script

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show startup-config {include-factory}
```

Parameters

```
show startup-config {include-factory}
```

startup-config include-factory	Displays startup configuration script • include-factory – Optional. Includes factory defaults

Example

```
rfs4000-229D58(config)#show startup-config
!
! Configuration of Brocade Mobility RFS4000 version 5.5.0.0-036B
!
!
version 2.3
!
!
client-identity TestClientIdentity
 dhcp 1 message-type request option-codes exact hexstring 5e4d36780b3a7f
!
client-identity-group ClientIdentityGroup
 client-identity TestClientIdentity precedence 1
!
alias network testNetworkAlias address-range 192.168.13.4 to 192.168.13.10
!
ip access-list BROADCAST-MULTICAST-CONTROL
 permit tcp any any rule-precedence 10 rule-description "permit all TCP
traffic"
 permit udp any eq 67 any eq dhcpc rule-precedence 11 rule-description "permit
DHCP replies"
 deny udp any range 137 138 any range 137 138 rule-precedence 20
rule-description "deny windows netbios"
 deny ip any 224.0.0.0/4 rule-precedence 21 rule-description "deny IP
multicast"
 deny ip any host 255.255.255.255 rule-precedence 22 rule-description "deny IP
l
--More--
rfs4000-229D58(config)#
```

terminal

show commands

Displays terminal configuration parameters

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show terminal
```

Parameters

None

Example

```
rfs7000-37FABE(config)#show terminal
Terminal Type: xterm
Length: 24     Width: 200
rfs7000-37FABE(config)#
```

timezone

show commands

Displays a device's timezone

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show timezone
```

Parameters

None

Example

```
rfs7000-37FABE(config)#show timezone
Timezone is America/Los_Angeles
rfs7000-37FABE(config)#
```

upgrade-status

show commands

Displays the last image upgrade status

NOTE
This command is not available in the USER EXEC Mode.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show upgrade-status {detail|on}
show upgrade-status {detail} {(on <DEVICE-NAME>)}
```

Parameters

```
show upgrade-status {detail} {(on <DEVICE-NAME>)}
```

upgrade-status	Displays last image upgrade status and log
detail	Optional. Displays last image upgrade status in detail
on <DEVICE-NAME>	The following keyword is recursive and common to the 'detail' parameter: • on <DEVICE-NAME> – Optional. Displays last image upgrade status on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Example

```
rfs4000-229D58(config)#show upgrade-status on rfs4000-229D58
Last Image Upgrade Status : Successful
Last Image Upgrade Time   : 2013-04-10 09:10:05
rfs4000-229D58(config)#

rfs4000-229D58(config)#show upgrade-status detail on rfs4000-229D58
Last Image Upgrade Status : Successful
Last Image Upgrade Time   : 2013-04-10 09:10:05
-----------------------------------------------
Running from partition /dev/mtdblock7
var2 is 3 percent full
/tmp is 5 percent full
Free Memory 114440 kB
FWU invoked via Linux shell
Validating image file header
Making file system
Extracting files (this may take some time).
Control C disabled
Version of firmware update file is 5.5.0.0-034B
Writing Kernel to /dev/mtd4
Writing BootOS to /dev/mtd2
Successful

rfs4000-229D58(config)#
```

version

show commands

Displays a device's software and hardware version

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show version {on <DEVICE-NAME>}
```

Parameters

```
show version {on <DEVICE-NAME>}
```

version {on <DEVICE-NAME>}	Displays software and hardware versions on all devices or a specified device • on <DEVICE-NAME> – Optional. Displays software and hardware versions on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Example

```
rfs4000-229D58(config)#show version
Brocade Mobility RFS4000 version 5.5.0.0-018D
Copyright (c) 2004-2013 Brocade Communications, Inc. All rights reserved.
Booted from primary

rfs4000-229D58 uptime is 14 days, 03 hours 55 minutes
CPU is Cavium Networks Octeon CN50XX V0.1
Base ethernet MAC address is 00-23-68-22-9D-58
System serial number is 9184521800027
Model number is RFS-4010-00010-WR
PoE firmware version is 211 build 1
FPGA version is 2.28
Radio HAL version is 92 (DFS:73)

rfs4000-229D58(config)#
```

vrrp

show commands

Displays *Virtual Router Redundancy Protocol* (VRRP) protocol details

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show vrrp [brief|details|error-stats|stats]
show vrrp [brief|details|stats] {<1-255>} {(on <DEVICE-NAME>)}
show vrrp error-stats {on <DEVICE-NAME>}
```

Parameters

```
show vrrp [brief|details|stats] {<1-255>} {(on <DEVICE-NAME>)}
```

brief	Displays virtual router information in brief
details	Displays virtual router information in detail

stats	Displays virtual router statistics
<1-255>	The following keyword is common to all of the above parameters: • <1-255> – Optional. Displays information for a specified Virtual Router. Specify the router's ID from 1 -255.
on <DEVICE-NAME>	The following keyword is recursive and common to the '<1-255>' parameter: • on <DEVICE-NAME> – Optional. Displays specified router information on a specified device <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
show vrrp error-stats {on <DEVICE-NAME>}
```

error-stats {on <DEVICE-NAME>}	Displays global error statistics • on <DEVICE-NAME> – Optional. Displays global error statistics on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Example

```
rfs7000-37FABE(config)#show vrrp error-stats on rfs7000-37FABE
Last protocol error reason: none
IP TTL errors: 0
Version mismatch: 0
Packet Length error: 0
Checksum error: 0
Invalid virtual router id: 0
Authentication mismatch: 0
Invalid packet type: 0
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show vrrp details on rfs7000-37FABE
VRRP Group 1:
  version 2
  interface none
  configured priority 1
  advertisement interval 1 sec
  preempt enable, preempt-delay 0
  virtual mac address 00-00-5E-00-01-01
  sync group disable
rfs7000-37FABE(config)#
```

what

show commands

Displays details of a specified search phrase (performs global search)

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show what [contain|is] <WORD> {on <DEVICE-OR-DOMAIN-NAME>}
```

Parameters

`show what [contain|is] <WORD> {on <DEVICE-OR-DOMAIN-NAME>}`

contain <WORD>	Searches on all the items that contain a specified word • <WORD> – Specify a word to search (for example, MAC address, hostname etc.).
is <WORD>	Searches on an exact match • <WORD> – Specify a word to search (for example, MAC address, hostname etc.).
on <DEVICE-OR-DOMAIN-NAME>	Optional. Performs global search on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

Example

```
rfs4000-229D58#show what contain default
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
NO. CATEGORY           MATCHED                    OTHER KEY INFO (1)
OTHER KEY INFO (2)             OTHER KEY INFO (3)
                      NAME/VALUE                 NAME/VALUE
NAME/VALUE                     NAME/VALUE
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------

                      https-trustpoint            type
mac                            rf_domain_name
1   device-cfg         default-trustpoint          rfs4000
00-23-68-22-9D-58              default

            __obj_name__          name
2 firewall_policy   default          default

                      __obj_name__                name
https                          idle_session_timeout
3   management_policy    default                    default
True                           30

                      qos_policy                  name
control_vlan                   beacon_format

--More--
rfs4000-229D58#
```

wireless

show commands

Displays wireless configuration parameters

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show wireless
[br|client|meshpoint|mobility-database|radio|regulatory|rf-domain|
          sensor-server|unsanctioned|wips|wlan]

show wireless br {configured|detail|load-balancing|on <DEVICE-NAME>}
show wireless br {configured}
show wireless br {detail} {<MAC/HOST-NAME>} {(on <DEVICE-OR-DOMAIN-NAME>)}
show wireless br {load-balancing} {client-capability|events|neighbors}
          {(on <DEVICE-NAME>)}

show wireless client {association-history|detail|filter|on
<DEVICE-OR-DOMAIN-NAME>|
          statistics|tspec}

show wireless client {association-history <MAC>} {on <DEVICE-OR-DOMAIN-NAME>}

show wireless client {detail <MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}

show wireless client {filter [ip|on|state|wlan]}
show wireless client {filter} {ip [<IP>|not <IP>]} {on
<DEVICE-OR-DOMAIN-NAME>}
show wireless client {filter} {on <DEVICE-OR-DOMAIN-NAME>}
show wireless client {filter} {state [data-ready|not
[data-ready|roaming]|roaming]}
          {on <DEVICE-OR-DOMAIN-NAME>}
show wireless client {filter} {wlan [<WLAN-NAME>|not <WLAN-NAME>]}
          {on <DEVICE-OR-DOMAIN-NAME>}

show wireless client {statistics} {detail|on|rf|window-data}
show wireless client {statistics} {detail <MAC>|rf|window-data <MAC>}
          {(on <DEVICE-OR-DOMAIN-NAME>)}

show wireless client {tspec <MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}

show wireless meshpoint {config|detail|multicast|neighbor|on|path|proxy|root|
          security|statistics|tree|usage-mappings}
show wireless meshpoint {config} {filter [device <DEVICE-NAME>|
          rf-domain <DOMAIN-NAME>]}
show wireless meshpoint {detail} {<MESHPOINT-NAME>}
show wireless meshpoint {on <DEVICE-OR-DOMAIN-NAME>}
show wireless meshpoint {multicast|path|proxy|root|security|statistics}
          [<MESHPOINT-NAME>|detail] {on <DEVICE-OR-DOMAIN-NAME>}
show wireless meshpoint neighbor [<MESHPOINT-NAME>|detail|statistics {rf}]
          {on <DEVICE-OR-DOMAIN-NAME>}
show wireless meshpoint {tree} {on <DEVICE-OR-DOMAIN-NAME>}
show wireless meshpoint {usage-mappings}

show wireless mobility-database {on <DEVICE-NAME>}

show wireless radio {detail|on
<DEVICE-OR-DOMAIN-NAME>|statistics|tspec|wlan-map}
show wireless radio {detail} {<DEVICE-NAME>|filter|on <DEVICE-OR-DOMAIN-NAME>}
show wireless radio {detail} {<DEVICE-NAME> {<1-3>|filter|on}}
show wireless radio {detail} {filter <RADIO-MAC>} {(on
<DEVICE-OR-DOMAIN-NAME>)}
show wireless radio {statistics} {detail|on|rf|windows-data}
show wireless radio {statistics} {on <DEVICE-OR-DOMAIN-NAME>|
          rf {on <DEVICE-OR-DOMAIN-NAME>}}
```

```
show wireless radio {statistics} {detail|window-data} {<DEVICE-NAME>} {<1-3>|
          filter <RADIO-MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}
show wireless radio {tspec} {<DEVICE-NAME>|filter|on
<DEVICE-OR-DOMAIN-NAME>|option}
show wireless radio {wlan-map} {on <DEVICE-OR-DOMAIN-NAME>}

show wireless regulatory [channel-info <WORD>|country-code <WORD>|device-type]
show wireless regulatory device-type
[br650|br6511|br1220|br7131|br71xx|rfs4000|rfs6000|rfs7000] <WORD>

show wireless rf-domain statistics {detail} {(on <DEVICE-OR-DOMAIN-NAME>)}

show wireless sensor-server {on <DEVICE-OR-DOMAIN-NAME>}

show wireless unsanctioned aps {detail|statistics} {(on
<DEVICE-OR-DOMAIN-NAME>)}

show wireless wips [client-blacklist|event-history] {on
<DEVICE-OR-DOMAIN-NAME>}

show wireless wlan {config|detail <WLAN>|on
<DEVICE-OR-DOMAIN-NAME>|policy-mappings|
          statistics|usage-mappings}
show wireless wlan {detail <WLAN>|on <DEVICE-OR-DOMAIN-NAME>|policy-mappings|
          usage-mappings}
show wireless {config filter {device <DEVICE-NAME>|rf-domain <DOMAIN-NAME>}}
show wireless wlan statistics {<WLAN>|detail|traffic} {on
<DEVICE-OR-DOMAIN-NAME>}
```

Parameters

`show wireless br {configured}`

wireless	Displays wireless configuration parameters
br	Displays managed access point information
configured	Optional. Displays configured AP information, such as name, MAC address, profile, RF Domain and adoption status

`show wireless br {detail} {<MAC/HOST-NAME>} {(on <DEVICE-OR-DOMAIN-NAME>)}`

wireless	Displays wireless configuration parameters
br	Displays managed access point information
detail <MAC/HOST-NAME>	Optional. Displays detailed information for all APs or a specified AP • <MAC/HOST-NAME> – Optional. Displays information for a specified AP
on <DEVICE-OR-DOMAIN-NAME>}	The following keyword is recursive and common to the 'detail <MAC/HOST-NAME>' parameter: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays information on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

`show wireless br {load-balancing} {client-capability|events|neighbors} {(on <DEVICE-NAME)}`

wireless	Displays wireless configuration parameters
br	Displays managed access point information

load-balancing {client-capability|events|neighbors}	Optional. Displays load balancing status. Use additional filters to view specific details. • client-capability – Optional. Displays client band capability • events – Optional. Displays client events • neighbors – Optional. Displays neighboring clients
on <DEVICE-NAME>	The following keyword is recursive and common to the 'client-capability', 'events', and 'neighbors' parameters: • on <DEVICE-NAME> – Optional. Displays load balancing information, based on the parameters passed, on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

`show wireless client {association-history <MAC>} {on <DEVICE-OR-DOMAIN-NAME>}`

wireless	Displays wireless configuration parameters
client	Displays client information based on the parameters passed
association-history <MAC>	Optional. Displays association history for a specified client • <MAC> – Specify the MAC address of the client.
on <DEVICE-OR-DOMAIN-NAME>	Optional. Displays association history on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

`show wireless client {detail <MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}`

wireless	Displays wireless configuration parameters
client	Displays client information based on the parameters passed
detail <MAC>	Optional. Displays detailed wireless client(s) information • <MAC> – Optional. Displays detailed information for a specified wireless client. Specify the MAC address of the client.
on <DEVICE-OR-DOMAIN-NAME>	The following keyword is recursive and common to the 'detail <MAC>' parameter: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays detailed information on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

`show wireless client {filter ip [<IP>|not <IP>]} {on <DEVICE-OR-DOMAIN-NAME>}`

wireless	Displays wireless configuration parameters
client	Displays client information based on the parameters passed
filter IP [<IP>|not <IP>]	Optional. Uses IP addresses to filter wireless clients • <IP> – Selects clients with IP address matching the <IP> parameter • not <IP> – Inverts the match selection
on <DEVICE-OR-DOMAIN-NAME>	The following keyword is common to the 'IP' and 'not IP' parameters: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays selected wireless client information on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

`show wireless client {filter} {state [data-ready|not [data-ready|roaming]|roaming]} {on <DEVICE-OR-DOMAIN-NAME>}`

wireless	Displays wireless configuration parameters
client	Displays client information based on the parameters passed

filter state [data-ready| not [data-ready| roaming]| roaming]	Optional. Filters clients based on their state • data-ready – Selects wireless clients in the data-ready state • not [data-ready|roaming] – Inverts match selection. Selects wireless clients neither ready nor roaming • Roaming – Selects roaming clients
on <DEVICE-OR-DOMAIN-NAME>	The following keyword is common to the 'ready', 'not', and 'roaming' parameters: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays selected client details on a specified device or RF Domain

`show wireless client {filter} {wlan [<WLAN-NAME>|not <WLAN-NAME>]} {on <DEVICE-OR-DOMAIN-NAME>}`

wireless	Displays wireless configuration parameters
client	Displays client information based on the parameters passed
filter wlan [<WLAN-NAME>| not <WLAN-NAME>]	Optional. Filters clients on a specified WLAN • <WLAN-NAME> – Specify the WLAN name. • not <WLAN-NAME> – Inverts the match selection
on <DEVICE-OR-DOMAIN-NAME>	The following keyword is common to the 'WLAN and 'not' parameters: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Filters clients on a specified device or RF Domain

`show wireless client {statistics} {detail <MAC>|rf|window-data <MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}`

wireless	Displays wireless configuration parameters
client	Displays client information based on the parameters passed
statistics {detail <MAC>|rf| window-data <MAC>}	Optional. Displays detailed client statistics. Use additional filters to view specific details. • detail <MAC> – Optional. Displays detailed client statistics • <MAC> – Optional. Displays detailed statistics for a specified client. Specify the client's MAC address. • rf – Optional. Displays detailed client statistics on a specified device or RF Domain • window-data <MAC> – Optional. Displays historical data, for a specified client • <MAC> – Optional. Specify the client's MAC address
on <DEVICE-OR-DOMAIN-NAME>	The following keyword is recursive and common to the 'detail <MAC>', 'RF', and 'window-data <MAC>' parameters: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays client statistics, based on the parameters passed, on a specified device or RF Domain

`show wireless client {tspec} {<MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}`

wireless	Displays wireless configuration parameters
client	Displays client information based on the parameters passed
tspec <MAC>	Optional. Displays detailed *traffic specification* (TSPEC) information for all clients or a specified client • <MAC> – Optional. Displays detailed TSPEC information for a specified client. Specify the MAC address of the client.
on <DEVICE-OR-DOMAIN-NAME>	The following keyword is recursive and common to the 'tspec <MAC>' parameter: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays detailed TSPEC information for wireless clients on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

`show wireless meshpoint {config} {filter [device <DEVICE-NAME>|rf-domain <DOMAIN-NAME>]}`

wireless	Displays wireless configuration parameters
meshpoint	Displays meshpoint related information
config	Optional. Displays all meshpoint configuration
filters [device <DEVICE-NAME>| rf-domain <DOMAIN-NAME>]	Optional. Provides additional filter options, such as device name and RF Domain name. • device <DEVICE-NAME> – Displays meshpoints applied to a specified device • <DEVICE-NAME> – Specify the device name • rf-domain <DOMAIN-NAME> – Displays meshpoints applied to a specified RF Domain • <DOMAIN-NAME> – Specify the domain name

`show wireless meshpoint {detail} {<MESHPOINT-NAME>}`

wireless	Displays wireless configuration parameters
meshpoint	Displays meshpoint related information
detail <MESHPOINT-NAME>	Optional. Displays detailed information for all meshpoints or a specified meshpoint • <MESHPOINT-NAME> – Optional. Displays detailed information for a specified meshpoint. Specify the meshpoint name.

`show wireless meshpoint {multicast|path|proxy|root|security|statistics} [<MESHPOINT-NAME>|detail] {on <DEVICE-OR-DOMAIN-NAME>}`

wireless	Displays wireless configuration parameters
meshpoint	Displays meshpoint related information
multicast	Optional. Displays meshpoint multicast information
path	Optional. Displays meshpoint path information
proxy	Optional. Displays meshpoint proxy information
root	Optional. Displays meshpoint root information
security	Optional. Displays meshpoint security information
statistics	Optional. Displays meshpoint statistics
[<MESHPOINT-NAME>| detail]	The following keywords are common to all of the above parameters: • <MESHPOINT-NAME> – Displays meshpoint related information for a specified meshpoint. Specify the meshpoint name. • detail – Displays detailed multicast information for all meshpoints
on <DEVICE-OR-DOMAIN-NAME>	The following keyword is common to all of the above parameters: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays detailed multicast information on a specified device or RF Domain.

`show wireless meshpoint {neighbor} [<MESHPOINT-NAME>|detail|statistics {rf}] {on <DEVICE-OR-DOMAIN-NAME>}`

wireless	Displays wireless configuration parameters
neighbor	Optional. Displays meshpoint neighbor information, based on the parameters passed

[<MESHPOINT-NAME>| detail|statistics {rf}]	Select one of the following parameter to view neighbor related information • <MESHPOINT-NAME> – Displays detailed multicast information for a specified meshpoint. Specify the meshpoint name. • detail – Displays detailed multicast information for all meshpoints • statistics – Displays neighbors related statistics • rf – Optional. Displays RF related statistics for neighbors
on <DEVICE-OR-DOMAIN-NAME>	The following keyword is common to all of the above parameters: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays meshpoint neighbor information, based on the parameters passed, on a specified device or RF Domain.

`show wireless meshpoint {tree} {on <DEVICE-OR-DOMAIN-NAME>}`

wireless	Displays wireless configuration parameters
meshpoint	Displays meshpoint related information **NOTE:** The *show* > *wireless* > *meshpoint* > *tree* command can be executed only from a wireless controller.
tree	Optional. Displays meshpoint network tree
on <DEVICE-OR-DOMAIN-NAME>	Optional. Displays meshpoint network tree on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Optional. Specify the name of AP, wireless controller, service platform, or RF Domain

`show wireless meshpoint {usage-mappings|on <DEVICE-OR-DOMAIN-NAME>}`

wireless	Displays wireless configuration parameters
meshpoint	Displays meshpoint related information
usgae-mappings	Optional. Lists all devices and profiles using the meshpoint
on <DEVICE-OR-DOMAIN-NAME>	Optional. Displays meshpoint applied to a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Optional. Specify the name of AP, wireless controller,service platform, or RF Domain

`show wireless mobility-database {on <DEVICE-NAME>}`

wireless	Displays wireless configuration parameters
mobility-database	Displays controller-assisted mobility database
on <DEVICE-OR-DOMAIN-NAME>	The following keyword is recursive and common to the 'filter <RADIO-MAC>' parameter: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays detailed radio operation status for all or a specified radio on a specified device or RF Domain.

`show wireless radio {detail} {<DEVICE-NAME> {<1-3>|filter|on}}`

wireless	Displays wireless configuration parameters
radio	Displays radio operation status and other related information
detail	Optional. Displays detailed radio operation status
<DEVICE-NAME>	Optional. Displays detailed information for a specified radio. Specify the MAC address or hostname, or append the interface number to form the radio ID in the AA-BB-CC-DD-EE-FF:RX or HOSTNAME:RX format.
<1-3>	Optional. Specify the radio interface index from 1 - 3 (if not specified as part of the radio ID)

filter <RADIO-MAC>	Optional. Provides additional filters • <RADIO-MAC> – Optional. Filters based on the radio MAC address
on <DEVICE-OR-DOMAIN-NAME>	Optional. After specifying the radio MAC address, further refine the search by specifying a device or RF Domain. • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

`show wireless radio {detail} {filter <RADIO-MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}`

wireless	Displays wireless configuration parameters
radio	Displays radio operation status and other related information
detail	Optional. Displays detailed radio operation status
filter <RADIO-MAC>	Optional. Provides additional filter options • <RADIO-MAC> – Uses MAC address to filter radios
on <DEVICE-OR-DOMAIN-NAME>	The following keyword is recursive and common to the 'filter <RADIO-MAC>' parameter: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays detailed radio operation status for all or a specified radio on a specified device or RF Domain.

`show wireless radio {statistics} {on <DEVICE-OR-DOMAIN-NAME>| rf {on <DEVICE-OR-DOMAIN-NAME>}}`

wireless	Displays wireless configuration parameters
radio	Displays radio operation status and other related information
statistics	Optional. Displays radio traffic and RF statistics
on <DEVICE-OR-DOMIAN-NAME>	Optional. Displays traffic and RF related statistics on a specified device or RF Domain • <DEVICE-OR-DOMIAN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.
rf {on <DEVICE-OR-DOMAIN-NAME>}	Optional. Displays RF statistics on a specified device or RF Domain • <DEVICE-OR-DOMIAN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

`show wireless radio {statistics} {detail|window-data} {<DEVICE-NAME>} {<1-3>| filter <RADIO-MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}`

wireless	Displays wireless configuration parameters
radio	Displays radio operation status and other related information
statistics {detail|window-data}	Optional. Displays radio traffic and RF statistics. Use additional filters to view specific details. The options are: are: • detail – Displays detailed traffic and RF statistics of all radios • window-data – Displays historical data over a time window
<DEVICE-NAME> <1-3>	The following keywords are common to the 'detail' and 'window-data' parameters: • <DEVICE-NAME> – Optional. Specify the MAC address or hostname, or append the interface number to form the radio ID in the AA-BB-CC-DD-EE-FF:RX or HOSTNAME:RX format. • <1-3> – Optional. Specify the radio interface index.
filter <RADIO-MAC>	Optional. Provides additional filters • <RADIO-MAC> – Optional. Filters based on the radio MAC address
on <DEVICE-OR-DOMAIN-NAME>	Optional. After specifying the radio MAC address, further refine the search by specifying a device or RF Domain. • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

`show wireless radio {tspec} {<DEVICE-NAME>|filter|on <DEVICE-OR-DOMAIN-NAME>| option}`

wireless	Displays wireless configuration parameters
radio	Displays radio operation status and other related information
tspec	Optional.Displays TSPEC information on a radio
<DEVICE-NAME>	Optional. Specify the MAC address or hostname, or append the interface number to form the radio ID in the AA-BB-CC-DD-EE-FF:RX or HOSTNAME:RX format.
filter	Optional. Provides additional filters • <RADIO-MAC> – Optional. Filters based on the radio MAC address
on <DEVICE-OR-DOMAIN-NAME>	Optional. After specifying the radio MAC address, further refine the search by specifying a device or RF Domain. • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

`show wireless regulatory [channel-info <WORD>|county-code <WORD>]`

wireless	Displays wireless configuration parameters
regulatory	Displays wireless regulatory information
channel-info <WORD>	Displays channel information • <WORD> – Specify the channel number.
country-code <WORD>	Displays country code to country name information • <WORD> – Specify the two letter ISO-3166 country code.

`show wireless regulatory device-type [br650|br6511|br1220| br7131|br71xx|br81xx|rfs4000|rfs6000|rfs7000] <WORD>`

wireless	Displays wireless configuration parameters
regulatory	Displays wireless regulatory information
device-type [br650|br6511|br1220|br71xx| br81xx|rfs4000| rfs6000|rfs7000] <WORD>	Displays regulatory information based on the device type • Brocade Mobility 650 Access Point – Displays Brocade Mobility 650 Access Point information • Brocade Mobility 6511 Access Point – Displays Brocade Mobility 6511 Access Point information • Brocade Mobility 1220 Access Point – Displays Brocade Mobility 1220 Access Point information • Brocade Mobility 7131 Access Point – Displays Brocade Mobility 7131 Access Point information • Brocade Mobility 71XX Access Point – Displays Brocade Mobility 71XX Access Point information • Brocade Mobility 1240 Access Point – Displays Brocade Mobility 1240 Access Point information • Brocade Mobility RFS4000 – Displays Brocade Mobility RFS4000 information • Brocade Mobility RFS6000 – Displays Brocade Mobility RFS6000 information • Brocade Mobility RFS7000 – Displays Brocade Mobility RFS7000 information The following keyword is common to all of the above: • <WORD> – Specify the two letter ISO-3166 country code.

`show wireless rf-domain statistics {detail} {(on <DEVICE-OR-DOMAIN-NAME>)}`

wireless	Displays wireless configuration parameters
rf-domain statistics	Displays RF Domain statistics
details	Optional. Displays detailed RF Domain statistics
on <DEVICE-OR-DOMAIN-NAME>	The following keyword is recursive and common to the 'detail' parameter: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays RF Domain statistics on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

show wireless sensor-server *{on <DEVICE-OR-DOMAIN-NAME>}*	
wireless	Displays wireless configuration parameters
sensor- server {on <DEVICE-OR-DOMAIN-NAME>}	Displays AirDefense sensor server configuration details • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays AirDefense sensor server configuration on a specified device or RF Domain

show wireless unsanctioned aps *{detailed|statistics} {(on <DEVICE-OR-DOMAIN-NAME>)}*	
wireless	Displays wireless configuration parameters
unsanctioned aps	Displays unauthorized APs. Use additional filters to view specific details.
detailed	Optional. Displays detailed unauthorized APs information
statistics	Optional. Displays channel statistics
on <DEVICE-OR-DOMAIN-NAME>	The following keyword is common to the 'detailed' and 'statistics' parameters: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Specify the name of the AP, wireless controller, service platform, or RF Domain.

show wireless wips [client-blacklist|event-history] *{on <DEVICE-OR-DOMAIN-NAME>}*	
wireless	Displays wireless configuration parameters
wips [client-blacklist|event-history]	Displays the WIPS details • client-blacklist – Displays blacklisted clients • event-history – Displays event history
on <DEVICE-OR-DOMAIN-NAME>	The following keyword is common to the 'client-blacklist' and 'event-history' parameters: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Specify the name of the AP, wireless controller, service platform, or RF Domain.

show wlan *{detail <WLAN>|on <DEVICE-OR-DOMAIN-NAME>|policy-mappings|usage-mappings}*	
wireless	Displays wireless configuration parameters
wlan	Displays WLAN related information based on the parameters passed
detail <WLAN>	Optional. Displays WLAN configuration • <WLAN> – Specify the WLAN name.
on <DEVICE-OR-DOMAIN-NAME>	Optional. Displays WLAN configuration on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.
policy-mappings	Optional. Displays WLAN policy mappings
usage-mappings	Optional. Lists all devices and profiles using the WLAN

show wlan *{config filter {device <DEVICE-NAME>|rf-domain <DOMAIN-NAME>}*	
wireless	Displays wireless configuration parameters
wlan	Displays WLAN related information based on the parameters passed
config filter	Optional. Filters WLAN information based on the device name or RF Domain

device <DEVICE-NAME>	Optional. Filters WLAN information based on the device name • <DEVICE-NAME> – Specify the device name.
rf-domain <DOMAIN-NAME>	Optional. Filters WLAN information based on the RF Domain • <DOMAIN-NAME> – Specify the RF Domain name.

`show wlan {statistics {<WLAN>|detail} {(on <DEVICE-OR-DOMAIN-NAME>)}`

wireless	Displays wireless configuration parameters
wlan	Displays WLAN related information based on the parameters passed
statistics {<WLAN>|detail}	Optional. Displays WLAN statistics. Use additional filters to view specific details • <WLAN> – Optional. Displays WLAN statistics. Specify the WLAN name. • detail – Optional. Displays detailed WLAN statistics
on <DEVICE-OR-DOMAIN-NAME>	The following keyword is common to the 'WLAN' and 'detail' parameters: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays WLAN statistics on a specified device or RF Domain

Usage Guidelines:

The customize command enables you to customize the *show* > *wireless* command output.

```
rfs7000-37FABE(config)#customize ?
  hostname-column-width                    Customize hostname column width
  show-wireless-client                     Customize the output of (show
                                           wireless client) command
  show-wireless-client-stats               Customize the output of (show
                                           wireless client stats) command
  show-wireless-client-stats-rf            Customize the output of (show
                                           wireless client stats rf)
  show-wireless-meshpoint                  Customize the output of (show
                                           wireless meshpoint) command
  show-wireless-meshpoint-neighbor-stats   Customize the output of (show
                                           wireless meshpoint neighbor
                                           stats) command
  show-wireless-meshpoint-neighbor-stats-rf Customize the output of (show
                                          wireless meshpoint neighbor stats
                                           rf) command
  show-wireless-radio                      Customize the output of (show
                                           wireless radio) command
  show-wireless-radio-stats                Customize the output of (show
                                           wireless radio stats) command
  show-wireless-radio-stats-rf             Customize the output of (show
                                           wireless radio stats rf) command

rfs7000-37FABE(config)#
```

The default setting for the *show* > *wireless* > *client* command is as follows:

```
rfs7000-37FABE(config)#show wireless client
-------------------------------------------------------------------------------
-----------------------------------
MAC           IP    VENDOR            RADIO-ID            WLAN
VLAN         STATE
-------------------------------------------------------------------------------
----------
-------------------------------------------------------------------------------
----------
Total number of wireless clients displayed: 0
rfs7000-37FABE(config)#
```

The above output can be customized, using the *customize* > *show-wireless-client* command, as follows:

```
rfs7000-37FABE(config)#customize show-wireless-client mac ip vendor vlan
radio-id state wlan location radio-alias radio-type
rfs7000-37FABE(config)#commit

rfs7000-37FABE(config)#show wireless client
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
--------
MAC                IP    VENDOR             VLAN  RADIO-ID             STATE
WLAN                 AP-LOCATION     RADIO                RADIO-TYPE
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
--------
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
--------
Total number of wireless clients displayed: 0
rfs7000-37FABE(config)#
```

For more information on the customize command, see *customize on page 4-216*.

Example

```
rfs7000-37FABE(config)#show wireless wips mu-blacklist
No mobile units blacklisted

rfs7000-37FABE(config)#show wireless wlan config
+-----------+---------+-----------+-------------+-----------------+-------
|    NAME   |  ENABLE |    SSID   |  ENCRYPTION |  AUTHENTICATION |    VLAN    |
+-----------+---------+-----------+-------------+-----------------+-------
| test      | Y       | test      | none        | none            | 1          |
| wlan1     | Y       | wlan1     | none        | none            | 1          |

rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show wireless wlan statistics
+---------------------+----------+----------+--------+--------+--------+--
|        WLAN         | TX BYTES | RX BYTES |TX PKTS |RX PKTS |TX KBPS |RX KBPS
|DROPPED |  ERRORS |
+---------------------+----------+----------+--------+--------+--------+-
|               wlan1 |        0 |        0 |      0 |      0 |      0 |      0
|      0 |      0  |
+---------------------+----------+----------+--------+--------+--------+--
Total number of wlan displayed: 2
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show wireless regulatory channel-info 1
Center frequency for channel 1 is 2412MHz
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show wireless regulatory country-code
ISO CODE                        NAME
-------------------------------------------------------------
  al                            Algeria
  ai                            Anguilla
  ar                            Argentina
  au                            Australia
  at                            Austria
```

```
  bs                          Bahamas
  bh                          Bahrain
  bb                          Barbados
  by                          Belarus
  be                          Belgium
  bm                          Bermuda
.....................................................
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show wireless regulatory device-type br650 in
------------------------------------------------------------------------------
-----------------------
 #  Channel Set Power(mW) Power (dBm)   Placement       DFS     CAC(mins)
TPC
------------------------------------------------------------------------------
----------
  1   1-13       1000     30         Indoor/Outdoor   NA            NA
NA
  2   36-64      200      23         Indoor          Not Required   0
Not Required
  3   149-165    1000     30         Outdoor         Not Required   0
Not Required
  4   149-165    200      23         Indoor          Not Required   0
Not Required
------------------------------------------------------------------------------
----------
rfs7000-37FABE(config)#

rfs4000-229D58(config)#show wireless br detail br7131-11E6C4 on rfs4000-229D58
AP: 00-23-68-11-E6-C4
 AP Name              : br7131-11E6C4
 Location             : default
 RF-Domain            : default
 Type                 : rfs4000
 Model                : RFS-4011-11110-US
 Num of radios        : 2
 Num of clients       : 0
 Last Smart-RF time   : not done
 Stats update mode    : auto
 Stats interval       : 6
 Radio Modes          :
     radio-1          : wlan
     radio-2          : wlan
 Country-code         : not-set
 Site-Survivable      : True
 Last error           :
 Fault Detected       : False
rfs4000-229D58(config)#

rfs4000-229D58(config)#show wireless br load-balancing on
default/rfs4000-229D58

AP: 00-23-68-11-E6-C4
Client requests on 5ghz   : allowed
Client requests on 2.4ghz : allowed

Average AP load in neighborhood              : 0 %
Load on this AP                              : 0 %
Total 2.4ghz band load in neighborhood       : 0 %
Total 5ghz band load in neighborhood         : 0 %
```

```
Configured band ratio 2.4ghz to 5ghz          : 1:1
Current band ratio 2.4ghz to 5ghz             : 0:0
Average 2.4ghz channel load in neighborhood   : 0 %
Average 5ghz channel load in neighborhood     : 0 %
Load on this AP's 2.4ghz channel              : 0 %
Load on this AP's 5ghz channel                : 0 %

Total number of APs displayed: 1
rfs4000-229D58(config)#

rfs4000-229D58(config)#show wireless br on default
-------------------------------------------------------------------------------
MODE       : radio modes - W = WLAN, S=Sensor, ' ' (Space) = radio not present
-------------------------------------------------------------------------------
AP-NAME    AP-LOCATION      RF-DOMAIN     AP-MAC   #RADIOS  MODE #CLIENT
LAST-CAL-TIME
-------------------------------------------------------------------------------
rfs4000-229D58   default    default 00-23-68-11-E6-C4  2  W-W    0
not done
-------------------------------------------------------------------------------
Total number of APs displayed: 1
rfs4000-229D58(config)#

rfs4000-1B3596#show wireless meshpoint tree
1:c00466 [5 MPs(3 roots, 2 bound)]
|-br7131-96FAAC
| |-br7131-96F998
|   |-br7131-96F6B4
|-ap622-7C0958
|-br650-33DF84

2:test [3 MPs(0 roots, 0 bound)]
*-br7131-96F998
*-br7131-96FAAC
*-br7131-96F6B4

Total number of meshes displayed: 2
rfs4000-1B3596#


rfs4000-1B3596#show wireless meshpoint
-------------------------------------------------------------------------------
-------------------------------------------------------------
MESH           HOSTNAME        HOPS IS-ROOT CONFIG-AS-ROOT ROOT-HOSTNAME
ROOT-BOUND-TIME NEXT-HOP-HOSTNAME NEXT-HOP-USE-TIME
-------------------------------------------------------------------------------
-------------------------------------------------------------
c00466          br7131-96F998       1 NO     NO           br7131-96FAAC
1 days 02:01:33 br7131-96FAAC       1 days 02:01:33
c00466         br7131-96FAAC      0 YES    YES         N/A
N/A N/A                            N/A
c00466          br7131-96F6B4       2 NO     NO           br7131-96FAAC
1 days 02:01:31 br7131-96F998       1 days 02:01:31
Total number of meshpoint displayed: 3
rfs4000-1B3596#

ap6532-000001#show wireless meshpoint multicast detail
Multicast Paths @00-23-68-00-00-01 (ap6532-000001), mesh1 [00-23-68-2E-64-B2]
-------------------------------------------------------------------------------
---
```

```
      Group-Addr      Subscriber Name    Subscriber MPID     Timeout (mSecs)
-------------------------------------------------------------------------------
---
01-00-5E-01-01-01   ap6532-000001     00-23-68-2E-64-B2   N/A
-------------------------------------------------------------------------------
---

Total number of meshpoint displayed: 1
ap6532-000001#

ap6532-000001#show wireless meshpoint neighbor detail
Neighbors @00-23-68-00-00-01 (ap6532-000001), mesh1 [00-23-68-2E-64-B2]
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
-
Neighbor Name          Neighbor MPID.IFID         Root Name     Root MPID
RMet Hops  Type      Interface       Auth-State Resourced Rank LQ% LMet Age
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
-
              5C-0E-8B-21-76-22.5C-0E-8B-21-74-40          00-23-68-2E-97-60
115  1    Fixed 00-23-68-00-00-01:R2 Enabled    Yes       0    97  87   20
              00-23-68-30-F7-82.00-23-68-30-F8-F0          00-23-68-2E-97-60
99   1    Fixed 00-23-68-00-00-01:R2 Init       Yes       0    97  86   30
              00-23-68-30-F7-82.00-23-68-30-F7-82          00-23-68-2E-97-60
99   1    Fixed 00-23-68-00-00-01:R1 Enabled    Yes       0    96  94   0
              5C-0E-8B-21-76-22.5C-0E-8B-21-76-22          00-23-68-2E-97-60
115  1    Fixed 00-23-68-00-00-01:R1 Enabled    Yes       0    96  93   30
              00-23-68-2E-AB-50.00-23-68-2E-AB-50          00-23-68-2E-AB-50
0    0    Root  00-23-68-00-00-01:R2 Enabled    Yes       7    96  87   40
              00-23-68-2E-97-60.00-23-68-2E-97-60          00-23-68-2E-97-60
0    0    Root  00-23-68-00-00-01:R2 Enabled    Yes       8    94  90   10
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
-

Total number of meshpoint displayed: 1
ap6532-000001#

ap6532-000001#show wireless meshpoint proxy detail
Proxies @00-23-68-00-00-01 (ap6532-000001), mesh1 [00-23-68-2E-64-B2]
-------------------------------------------------------------------------------
---
  Destination Addr   Owner Name      Owner MPID     Persist  VLAN      Age
-------------------------------------------------------------------------------
---
00-23-68-00-00-01 ap6532-000001 00-23-68-2E-64-B2 Permanent 101  180654310
00-1E-E5-A6-66-E2 ap6532-000001 00-23-68-2E-64-B2 Untimed   103  231920
-------------------------------------------------------------------------------
---

Total number of meshpoint displayed: 1
ap6532-000001#

ap6532-000001#show wireless meshpoint multicast mesh1 on ap6532-000001
Multicast Paths @00-23-68-00-00-01 (ap6532-000001), mesh1 [00-23-68-2E-64-B2]
-------------------------------------------------------------------------------
---
      Group-Addr      Subscriber Name    Subscriber MPID     Timeout (mSecs)
```

```
-------------------------------------------------------------------------------
---
01-00-5E-01-01-01   ap6532-000001     00-23-68-2E-64-B2   -1
-------------------------------------------------------------------------------
---

Total number of meshpoint displayed: 1
ap6532-000001#

ap6532-000001#show wireless meshpoint path detail
Paths @00-23-68-00-00-01 (ap6532-000001), mesh1 [00-23-68-2E-64-B2]
-------------------------------------------------------------------------------
-----------------------------------------------------------------
Destination Name  Destination Addr Next Hop Name   Next Hop IFID   State Hops
Type Binding Metric Timeout Path-Timeout Sequence     MiNT ID
-------------------------------------------------------------------------------
-----------------------------------------------------------------
                  00-23-68-2E-AB-50              00-23-68-2E-AB-50 Valid 1
Root Bound   89     8730    0            23847    68.31.19.58
                  00-23-68-2E-97-60              00-23-68-2E-97-60 Valid 1
Root Unbound 92     5200    0            3481     68.31.1A.80
-------------------------------------------------------------------------------
-----------------------------------------------------------------
ap6532-000001#

rfs4000-22A24E#show wireless client
-------------------------------------------------------------------------------
-----------------------------------
Report start on RF-Domain: qs1
MAC                   IP   VENDOR          RADIO-ID          WLAN
VLAN         STATE
-------------------------------------------------------------------------------
-----------------------------------
Report end on RF-Domain: qs1
-------------------------------------------------------------------------------
-----------------------------------

-------------------------------------------------------------------------------
-----------------------------------
Report start on RF-Domain: Store-1
MAC                   IP   VENDOR          RADIO-ID          WLAN
VLAN         STATE
-------------------------------------------------------------------------------
-----------------------------------
00-01-02-03-04-10        2.3.4.16 3Com Corp          00-01-02-03-04-00:R1
sim-wlan-1           1       Data-Ready
00-01-02-03-05-10        2.3.5.16 3Com Corp          00-01-02-03-04-00:R2
sim-wlan-1           1       Data-Ready
Report end on RF-Domain: Store-1
-------------------------------------------------------------------------------
-----------------------------------

-------------------------------------------------------------------------------
-----------------------------------
Report start on RF-Domain: default
  database not available
Report end on RF-Domain: default
-------------------------------------------------------------------------------
-----------------------------------
```

```
Total number of clients displayed: 2
rfs4000-22A24E#
```

wwan

show commands

Displays wireless WAN status

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show wwan [configuration|status] {on <DEVICE-OR-DOMAIN-NAME>}
```

Parameters

```
show wwan [configuration|status] {on <DEVICE-OR-DOMAIN-NAME>}
```

wwan	Displays wireless WAN configuration and status details
configuration	Displays wireless WAN configuration information
status	Displays wireless WAN status information
on <DEVICE-OR-DOMAIN-NAME>	The following keyword is common to the 'configuration' and 'status' parameters: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays configuration or status details on a specified device or RF Domain

Example

```
rfs4000-229D58(config-device-00-23-68-22-9D-58)#show wwan configuration on
rfs4000-229D58
>>> WWAN Configuration:
+-----------------------------------------
|  Access Port Name : isp.cingular
|  User Name        : testuser
|  Cryptomap        : map1
+-----------------------------------------
rfs4000-229D58(config-device-00-23-68-22-9D-58)#

rfs4000-229D58(config-device-00-23-68-22-9D-58)#show wwan status on
rfs4000-229D58
>>> WWAN Status:
+-----------------------------------------
|  State : ACTIVE
|  DNS1  : 209.183.54.151
|  DNS2  : 209.183.54.151
+-----------------------------------------
rfs4000-229D58(config-device-00-23-68-22-9D-58)#

rfs7000-37FABE(config)#show wwan configuration on rfs7000-37FABE
>>> WWAN Configuration:
```

```
+----------------------------------------
|  Access Port Name : None
|  User Name        : None
+----------------------------------------

rfs7000-37FABE(config)#
```

smart-cache

show commands

Displays details on the cached entry for a specific URL or all URLs

NOTE
Smart content caching is a licensed feature and can be enabled only if a license is procured and applied to the device. For more information, see *smart-cache-policy*.

Supported in the following platforms:

- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show smart-cache [active-requests|clients|purge-requests|statistics
content-type|
          storage] {on <DEVICE-NAME>}
```

Parameters

```
show smart-cache [active-requests|clients|purge-requests|statistics
content-type|
storage] {on <DEVICE-NAME>}
```

smart-cache	Displays smart-cache related information
active-requests	Displays all current in-progress requests
clients	Displays all clients since the boot-up
purge-requests	Displays all requests that have been purged (cleared)
statistics content-type	Displays detailed cached content statistics
storage	Displays storage statistics in KB
on <DEVICE-NAME>	Displays smart-cache related information on a specified device • <DEVICE-NAME> – Specify the name of the access point, wireless controller, or service platform.

Example

```
nx4500-5CFA2B>show smart-cache statistics
Warning: no smart-cache license installed, smart-cache is not running.
Warning: name-server not configured, smart-cache may not work!
-------------------------------------------------------------------------
--
    DURATION   |      DATA (KB)      | BANDWIDTH (Kbps)  |      REQUESTS
               |   TOTAL      CACHE  |   WAN      CACHE  |   TOTAL      CACHE
---------------|----------|----------|---------|---------|----------|--------
--
Since boot     |         0|         0|      0.0|      0.0|         0|         0
-------------------------------------------------------------------------
--
```

```
nx4500-5CFA2B>

nx4500-5CFA2B(config)#show smart-cache statistics content-type
------------------------------------------------------------------------------
-----------------------------------------------
    DURATION   |      VIDEO (KB)     |      AUDIO (KB)     |      IMAGE (KB)
|      TEXT  (KB)     |      OTHERS (KB)
               |   TOTAL      CACHE  |   TOTAL      CACHE  |   TOTAL      CACHE
|   TOTAL      CACHE  |   TOTAL      CACHE
---------------|----------|----------|----------|----------|----------|------
----|----------|----------|----------|----------
Since boot     |        0|        0|        0|        0|        0|        0|
0|         0|         0|         0
------------------------------------------------------------------------------
-----------------------------------------------
nx4500-5CFA2B(config)#


nx4500-5CFA2B#show smart-cache storage
------------------------------
  USED    TOTAL      USAGE
------------------------------
  0 MB   DISABLED   DISABLED
------------------------------
nx4500-5CFA2B#
```

virtual-machine

show commands

Displays the *virtual-machine* (VM) configuration, logs, and statistics

Supported in the following platforms:

- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
show virtual-machine [configuration|debugging|export|statistics]

show virtual-machine [configuration|statistics] {<VM-NAME>|team-urc|team-rls|
          team-vowlan} {(on <DEVICE-NAME>)}

show virtual-machine debugging {level|on}
show virtual-machine debugging {level [debug|error|info|warning]} {on
<DEVICE-NAME>}

show virtual-machine export <VM-NAME> {on <DEVICE-NAME>}

The Brocade Mobility RFS9510 series service platforms support ADSP and
TEAM-CMT virtual machines only. The following show commands are specific to
the Brocade Mobility RFS9510 devices:

show virtual-machine [configuration|statistics] {<VM-NAME>|adsp|team-cmt}
```

Parameters

`show virtual-machine [configuration|statistics] {<VM-NAME>|team-urc|team-rls|team-vowlan} {(on <DEVICE-NAME>)}`

configuration	Displays detailed VM configuration
statistics	Displays VM statistics
[<VM-NAME>| team-urc|team-rls| team-vowlan]	The following keywords are common to the 'configuration' and 'statistics' parameters: • <VM-NAME> – Optional. Displays VM configuration or statistics for the virtual machine identified by the <VM-NAME> keyword. Specify the VM name. • team-urc – Optional. Displays TEAM-URC (IP-PBX) VM configuration/statistics • team-rls – Optional. Displays TEAM-RLS (Radio Link Server) VM configuration/statistics • team-vowlan – Optional. Displays TEAM-VoWLAN (Voice over WLAN) VM configuration/statistics
on <DEVICE-NAME>	Specifies the name of the device on which the command is executed • <DEVICE-NAME> – Specify the name of the service platform.

`show virtual-machine [configuration|statistics] {<VM-NAME>|adsp|team-cmt} {(on <DEVICE-NAME>)}`

configuration	Displays detailed VM configuration
statistics	Displays VM statistics
[<VM-NAME>|adsp| team-cmt]	The following keywords are common to the 'configuration' and 'statistics' parameters: • <VM-NAME> – Optional. Displays VM configuration or statistics for the virtual machine identified by the <VM-NAME> keyword. Specify the VM name. • adsp – Optional. Displays *Air-Defense Services Platform* (ADSP) VM configuration/statistics • team-cmt – Optional. Displays TEAM-CMT VM configuration/statistics These keywords are specific to the Brocade Mobility RFS9510 service platforms.
on <DEVICE-NAME>	Specifies the name of the device on which the command is executed • <DEVICE-NAME> – Specify the name of the service platform.

`show virtual-machine debugging {level[debug|error|info|warning]} {on <DEVICE-NAME>}`

debugging	Displays VM logs
level [debug| error|info|warning]	Optional. Displays VM logs based on the level selected. The available options are: • debug – Displays VM logs of level debug and above • error – Displays VM logs of level error • info – Displays VM logs of level Info and above • warning – Displays logs of level warning and above The Brocade Mobility RFS9510 series service platforms will display ADSP and TEAM-CMT VM debugging logs.
on <DEVICE-NAME>	Specifies the name of the device on which the command is executed • <DEVICE-NAME> – Specify the name of the service platform.

`show virtual-machine export <VM-NAME> {on <DEVICE-NAME>}`

export	Displays VM configuration export related information
<VM-NAME>	Displays VM configuration export related information for the virtual machine identified by the <VM-NAME> keyword. Specify the VM name. The Brocade Mobility RFS9510 series service platforms will display ADSP and TEAM-CMT VM configuration export information
on <DEVICE-NAME>	Specifies the name of the device on which the command is executed • <DEVICE-NAME> – Specify the name of the service platform.

Example

```
nx4500-5CFA2B#show virtual-machine configuration team-urc
VM: team-urc
  autostart       : start
  bootloader      : /usr/bin/pygrub
  cpus            : ["3","2"]
  disk            : file:/vms/moto/team-centro/disk,xvda,w
  maxmem          : 3584 MB
  maxvcpus        : 2
  memory          : 1200 MB
  name            : team-urc
  on_crash        : coredump-restart
  on_poweroff     : destroy
  on_reboot       : restart
  serial          : pty
  tty             : /dev/pts/1
  uuid            : b80f8e19-a1f6-02c9-cbbc-10c1aeb0a170
  vcpus           : 1
  vif             : bridge=vm2br, mac=B4:C7:99:5C:FA:2F, script=vif-bridge,
type=bridge
                  : bridge=brpriv, mac=00:16:3e:65:ff:01, script=vif-bridge
                  : bridge=vm3br, mac=B4:C7:99:5C:FA:31, script=vif-bridge,
type=bridge
nx4500-5CFA2B#

nx4500-5CFA2B#show virtual-machine configuration
--------------------------------------------------------------------------------
---
          NAME              AUTOSTART           MEMORY(MB)          VCPUS
--------------------------------------------------------------------------------
---
  team-rls              start             512                1
  team-urc              start             1200               1
  team-vowlan           start             1500               1
--------------------------------------------------------------------------------
---
nx4500-5CFA2B#

nx4500-5CFA2B#show virtual-machine statistics
--------------------------------------------------------------------------------
---
      NAME           STATE       VCPUS MEM (MB)   BRIDGE-IF           IP
--------------------------------------------------------------------------------
---
  Mobility          -                 4     1009     -             -
  team-rls      (not_installed)   -     -        -               -
  team-urc      Running           1     1200     eth0 (vmif2)   192.168.13.103
  team-vowlan   (not_installed)   -     -        -               -
--------------------------------------------------------------------------------
---
nx4500-5CFA2B#
```

Chapter

PROFILES 7

Profiles enable administrators to assign a common set of configuration parameters, policies, WLANs, wireless parameters, and security parameters to service platforms, wireless controllers, and access points across a large, multi segment, site. The configuration parameters within a profile are based on the hardware model the profile was created to support.

The service platforms, wireless controllers, and access points support both default and user-defined profiles. Each default and user-defined profile contains policies and configurations that are applied to devices assigned to the profile. Changes made to these configurations are automatically inherited by the assigned devices. Therefore, the central benefit of a profile is its ability to update devices collectively without having to modify individual device configurations.

The system maintains a couple of default profiles. The default profile is automatically applied to service platforms and wireless controllers. The default AP profile is applied to a AP automatically discovered by a wireless controller or service platform. After adoption, if a change is made in one of the parameters in the profile, it is reflected across all devices using the profile. Default profiles are ideal for single site deployments where service platforms, wireless controllers, and access points share a common configuration.

User-defined profiles are manually created for each supported service platform, wireless controller, and access point model. Brocade recommends user-defined profiles in larger deployments when groups of devices (on different floors, buildings or sites) share a common configuration. These user-defined profiles can be manually or automatically assigned to access points using an AP auto provisioning policy. An AP auto provisioning policy provides the means to assign profiles to access points based on model, serial number, VLAN ID, DHCP options, IP address (subnet) and MAC address. For more information, see *Chapter 9, AUTO-PROVISIONING-POLICY*.

A user defined profile can be created for each of the following device type:

- Brocade Mobility 650 Access Point – Adds an Brocade Mobility 650 Access Point access point profile
- Brocade Mobility 6511 Access Point – Adds an Brocade Mobility 6511 Access Point access point profile
- Brocade Mobility 1220 Access Point – Adds an Brocade Mobility 1220 Access Point access point profile
- Brocade Mobility 71XX Access Point – Adds an Brocade Mobility 71XX Access Point access point profile
- Brocade Mobility 1240 Access Point – Adds an Brocade Mobility 1240 Access Point access point profile
- Brocade Mobility RFS4000 – Adds an Brocade Mobility RFS4000 wireless controller profile
- Brocade Mobility RFS6000 – Adds an Brocade Mobility RFS6000 wireless controller profile
- Brocade Mobility RFS7000 – Adds an Brocade Mobility RFS7000 wireless controller profile
- Brocade Mobility RFS9510 – Adds an service platform profile supporting the Brocade Mobility RFS9510 model

Although profiles assign a common set of configuration parameters across devices, individual devices can still be assigned unique configuration parameters that follow the flat configuration model. As individual device updates are made, these devices no longer share the profile based configuration they originally supported. Therefore, changes made to a profile are not automatically inherited by devices who have had their configuration customized. These devices require careful administration, as they cannot be tracked as profile members. Their customized configurations overwrite their profile configurations until the profile is re-applied.

NOTE
The commands present under 'Profiles' are also available under the 'Device mode'. The additional commands specific to the 'Device mode' are listed separately.

This chapter is organized into the following topics:

To view the list of device profiles supported, use the following command:

```
<DEVICE>(config)#profile ?
br650       Brocade Mobility 650 Access Point access point profile
br6511      Brocade Mobility 6511 Access Point access point profile
br1220      Brocade Mobility 1220 Access Point access point profile
br71xx      Brocade Mobility 71XX Access Point access point profile
br81xx      Brocade Mobility 1240 Access Point access point profile
containing  Specify profiles that contain a sub-string in the profile name
filter      Specify addition selection filter
rfs4000     Brocade Mobility RFS4000 wireless controller profile
rfs6000     Brocade Mobility RFS6000 wireless controller profile
rfs7000     Brocade Mobility RFS7000 wireless controller profile

<DEVICE>(config)#

rfs7000-37FABE(config)#profile rfs7000 default-rfs7000
rfs7000-37FABE(config-profile-default-rfs7000)#

rfs7000-37FABE(config)#profile br71xx default-br71xx
rfs7000-37FABE(config-profile-default-br71xx)#

<DEVICE>(config-profile-<PROFILE-NAME>)#?
Profile Mode commands:
  adopter-auto-provisioning-policy-lookup  Use centralized auto-provisioning
                                           policy when adopted by another
                                           controller
  alias                                    Alias
  area                                     Set name of area where the system
                                           is located
  arp                                      Address Resolution Protocol (ARP)
  auto-learn-staging-config                Enable learning network
                                           configuration of the devices that
                                           come for adoption
  autogen-uniqueid                         Autogenerate a unique id
  autoinstall                              Autoinstall settings
  bridge                                   Ethernet bridge
  captive-portal                           Captive portal
  cdp                                      Cisco Discovery Protocol
  cluster                                  Cluster configuration
  configuration-persistence                Enable persistence of configuration
                                           across reloads (startup config
```

```
                                                 file)
controller                                       WLAN controller configuration
critical-resource                                Critical Resource
crypto                                           Encryption related commands
device-upgrade                                   Device firmware upgrade
dot1x                                            802.1X
dscp-mapping                                     Configure IP DSCP to 802.1p
                                                 priority mapping for untagged
                                                 frames
email-notification                               Email notification configuration
enforce-version                                  Check the firmware versions of
                                                 devices before interoperating
environmental-sensor                             Environmental Sensors Configuration
events                                           System event messages
export                                           Export a file
floor                                            Set the floor within a area where
                                                 the system is located
gre                                              GRE protocol
http-analyze                                     Specify HTTP-Analysis configuration
interface                                        Select an interface to configure
ip                                               Internet Protocol (IP)
l2tpv3                                           L2tpv3 protocol
l3e-lite-table                                   L3e lite Table
led                                              Turn LEDs on/off on the device
led-timeout                                      Configure the time for the led to
                                                 turn off after the last radio state
                                                 change
legacy-auto-downgrade                            Enable device firmware to auto
                                                 downgrade when other legacy devices
                                                 are detected
legacy-auto-update                               Auto upgrade of legacy devices
lldp                                             Link Layer Discovery Protocol
load-balancing                                   Configure load balancing parameter
logging                                          Modify message logging facilities
mac-address-table                                MAC Address Table
mac-auth                                         802.1X
memory-profile                                   Memory profile to be used on the
                                                 device
meshpoint-device                                 Configure meshpoint device
                                                 parameters
meshpoint-monitor-interval                       Configure meshpoint monitoring
                                                 interval
min-misconfiguration-recovery-time               Check controller connectivity after
                                                 configuration is received
mint                                             MiNT protocol
misconfiguration-recovery-time                   Check controller connectivity after
                                                 configuration is received
neighbor-inactivity-timeout                      Configure neighbor inactivity
                                                 timeout
neighbor-info-interval                           Configure neighbor information
                                                 exchange interval
no                                               Negate a command or set its
                                                 defaults
noc                                              Configure the noc related setting
ntp                                              Ntp server A.B.C.D
power-config                                     Configure power mode
preferred-controller-group                       Controller group this system will
                                                 prefer for adoption
preferred-tunnel-controller                      Tunnel Controller Name this system
                                                 will prefer for tunneling extended
```

```
                                        vlan traffic
  radius                                Configure device-level radius
                                        authentication parameters
  raid                                  RAID
  rf-domain-manager                     RF Domain Manager
  router                                Dynamic routing
  slot                                  PCI expansion Slot
  spanning-tree                         Spanning tree
  tunnel-controller                     Tunnel Controller group this
                                        controller belongs to
  use                                   Set setting to use
  vrrp                                  VRRP configuration
  wep-shared-key-auth                   Enable support for 802.11 WEP
                                        shared key authentication


  clrscr                                Clears the display screen
  commit                                Commit all changes made in this
                                        session
  do                                    Run commands from Exec mode
  end                                   End current mode and change to EXEC
                                        mode
  exit                                  End current mode and down to
                                        previous mode
  help                                  Description of the interactive help
                                        system
  revert                                Revert changes
  service                               Service Commands
  show                                  Show running system information
  write                                 Write running configuration to
                                        memory or terminal

<DEVICE>(config-profile-<PROFILE-NAME>)#
```

Profile Config Commands

PROFILES

Table 5 summarizes profile configuration commands.

TABLE 5 Profile-Config Commands

Command	Description	Reference
adopter-auto-provisioning-policy-lookup	Enables the use of a centralized auto provisioning policy on this profile	page 545
alias	Configures network, network-group, network-service, VLAN, and string aliases on this profile	page 546
area	Sets the system's area of location (the area name)	page 551
arp	Configures static address resolution protocol	*page 7-552*
auto-learn-staging-config	Enables network configuration learning of devices	*page 7-553*
autogen-uniqueid	Autogenerates a unique local ID for devices using this profile. When executed in the device configuration mode, this command generates a unique ID for the logged device	page 554
autoinstall	Configures the automatic install feature	*page 7-556*

TABLE 5 Profile-Config Commands

Command	Description	Reference
bridge	Configures bridge specific parameters	*page 7-557*
captive-portal	configures captive portal advanced Web page upload on a device profile	*page 7-572*
cdp	Enables *Cisco Discovery Protocol* (CDP) on a device	*page 7-573*
cluster	Configures a cluster name	*page 7-574*
configuration-persistence	Enables persistence of configuration across reloads	*page 7-576*
controller	Configures a wireless controller or service platform	*page 7-577*
critical-resource	Monitors user configured IP addresses and logs their status	*page 7-580*
crypto	Configures data encryption related protocols and settings	*page 7-583*
device-upgrade	Configures device firmware upgrade settings on this profile	page 631
dot1x	Configures 802.1x standard authentication controls	page 634
dscp-mapping	Configures an IP DSCP to 802.1p priority mapping for untagged frames	*page 7-635*
email-notification	Configures e-mail notification	*page 7-636*
enforce-version	Enables checking of a device's firmware version before attempting adoption or clustering	*page 7-638*
environmental-sensor	Configures the environmental sensor settings on this profile	page 639
events	Displays system event messages	*page 7-641*
export	Enables export of startup.log file after every boot	page 642
floor	Sets the floor name where the system is located	page 643
gre	Enables *Generic Routing Encapsulation* (GRE) tunneling on this profile	page 644
http-analyze	Configures HTTP analysis settings	page 652
interface	Configures an interface (VLAN, radio, GE etc.)	page 653
ip	Configures IP components	*page 7-744*
l2tpv3	Defines the *Layer 2 Tunnel Protocol* (L2TP) protocol for tunneling layer 2 payloads using *Virtual Private Networks* (VPNs)	*page 7-752*
l3e-lite-table	Configures L3e Lite Table with this profile	*page 7-753*
led	Turns device LEDs on or off	*page 7-754*
led-timeout	Configures LED-timeout timer. This command is specific to the NX9000 series service platforms.	*led-timeout*
legacy-auto-downgrade	Auto downgrades a legacy device firmware	*page 7-756*
legacy-auto-update	Auto upgrades a legacy device firmware	*page 7-757*
lldp	Configures *Link Layer Discovery Protocol* (LLDP)	*page 7-757*
load-balancing	Configures load balancing parameters	*page 7-759*
logging	Modifies message logging	*page 7-763*
mac-address-table	Configures the MAC address table	*page 7-764*
mac-auth	Enables 802.1x user authentication protocol on this profile	*page 7-766*
memory-profile	Configures the memory profile used on the device	page 769

TABLE 5 Profile-Config Commands

Command	Description	Reference
meshpoint-device	Configures a meshpoint device parameters	page 770
meshpoint-monitor-interval	Configures meshpoint monitoring interval	page 770
min-misconfiguration-recovery-time	Configures the minimum device connectivity verification time	page 771
mint	Configures MiNT protocol	*page 7-772*
misconfiguration-recovery-time	Verifies device connectivity after a configuration is received	*page 7-775*
neighbor-inactivity-timeout	Configures neighbor inactivity timeout	*page 7-776*
neighbor-info-interval	Configures neighbor information exchange interval	*page 7-777*
no	Negates a command or reverts settings to their default	*page 7-778*
noc	Configures NOC settings	*page 7-780*
ntp	Configures an NTP server	*page 7-781*
power-config	Configures the power mode	*page 7-783*
preferred-controller-group	Specifies the wireless controller or service platform group preferred for adoption	*page 7-784*
preferred-tunnel-controller	Configures the tunnel wireless controller or service platform preferred by the system to tunnel extended VLAN traffic	*page 7-785*
radius	Configures device-level RADIUS authentication parameters	*page 7-786*
rf-domain-manager	Enables RF Domain manager	*page 7-787*
router	Configures dynamic router protocol settings	*page 7-788*
spanning-tree	Configures spanning tree commands	*page 7-789*
tunnel-controller	Configures the name of tunneled WLAN (extended VLAN) wireless controller or service platform	*page 7-791*
use	Uses pre configured policies with this profile	*page 7-792*
vrrp	Configures *Virtual Router Redundancy Protocol* (VRRP) group settings	*page 7-795*
wep-shared-key-auth	Enables support for 802.11 WEP shared key authentication	*page 7-798*
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug (config-if) instance configurations	page 799
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

adopter-auto-provisioning-policy-lookup

Profile Config Commands

Enables the use of a centralized auto provisioning policy on this profile or device

When applied on devices adopted by a controller, this profile allows the devices to use a centralized auto provisioning policy.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
use-adopter-auto-provisioning-policy-lookup
```

Parameters

None

Example

```
rfs4000-229D58(config-profile-testBrocade Mobility
RFS4000)#adopter-auto-provisioning-policy-lookup
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000)#

rfs4000-229D58(config-profile-testBrocade Mobility RFS4000)#show context
profile rfs4000 testBrocade Mobility RFS4000
 bridge vlan 1
  tunnel-over-level2
  ip igmp snooping
  ip igmp snooping querier
 no autoinstall configuration
 no autoinstall firmware
 device-upgrade persist-images
 ..................................................................
  qos trust 802.1p
 interface ge4
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge5
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface wwan1
 interface pppoe1
 use firewall-policy default
 service pm sys-restart
 use-adopter-auto-provisioning-policy
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000)#
```

Related Commands:

no	Removes the use of centralized auto provisioning policy on this profile or device

alias

Profile Config Commands

Configures network, VLAN, and service aliases. The aliases defined on this profile applies to all devices using this profile.

Aliases can be also defined at the device level.

NOTE
You can apply overrides to aliases at the device level. For more information on aliases, see *alias*. Overrides applied at the device level take precedence.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
alias [address-range|host|network|network-group|network-service|string|vlan]

alias address-range <ADDRESS-RANGE-ALIAS-NAME> <STARTING-IP> to <ENDING-IP>

alias host <HOST-ALIAS-NAME> <HOST-IP>

alias network <NETWORK-ALIAS-NAME> <NETWORK-ADDRESS/MASK>

alias network-group <NETWORK-GROUP-ALIAS-NAME> [address-range|host|network]
alias network-group <NETWORK-GROUP-ALIAS-NAME> [address-range <STARTING-IP> to
          <ENDING-IP> {<STARTING-IP> to <ENDING-IP>}|host <HOST-IP>
{<HOST-IP>}|
          network <NETWORK-ADDRESS/MASK> {<NETWORK-ADDRESS/MASK>}]

alias network-service <NETWORK-SERVICE-ALIAS-NAME> proto
[<0-254>|<WORD>|eigrp|gre|
          igmp|igp|ospf|vrrp]
{(<1-65535>|<WORD>|bgp|dns|ftp|ftp-data|gopher|https|ldap|nntp|
          ntp|pop3|proto|sip|smtp|sourceport|ssh|telnet|tftp|www)}

alias network-service <NETWORK-SERVICE-ALIAS-NAME> proto
[<0-254>|<WORD>|eigrp|gre|
          igmp|igp|ospf|vrrp]
{(<1-65535>|<WORD>|bgp|dns|ftp|ftp-data|gopher|https|ldap|nntp|
          ntp|pop3|proto|sip|smtp|sourceport
[<1-65535>|<WORD>]|ssh|telnet|tftp|www)}

alias string <STRING-ALIAS-NAME> <LINE>
```

```
alias vlan <VLAN-ALIAS-NAME> <1-4094>
```

Parameters

```
alias address-range <ADDRESS-RANGE-ALIAS-NAME> <STARTING-IP> to <ENDING-IP>
```

address-range <ADRESS-RANGE-ALIAS-NAME>	Creates a new address-range alias for this profile. Or associates an existing address-range alias with this profile. An address-range alias maps a name to a range of IP addresses. • <ADRESS-RANGE-ALIAS-NAME> – Specify the address range alias name. Alias name should begin with '$'.
<STARTING-IP> to <ENDING-IP>	Associates a range of IP addresses with this address range alias • <STARTING-IP> – Specify the first IP address in the range. • to <ENDING-IP> – Specify the last IP address in the range. If using an existing address-range alias, you can apply overrides to the alias at the profile level.

```
alias host <HOST-ALIAS-NAME> <HOST-IP>
```

host <HOST-ALIAS-NAME>	Creates a new host alias for this profile. Or associates an existing host alias with this profile. A host alias maps a name to a single network host. • <HOST-ALIAS-NAME> – Specify the host alias name. Alias name should begin with '$'.
<HOST-IP>	Associates the network host's IP address with this host alias • <HOST-IP> – Specify the network host's IP address. If using an existing host alias, you can apply overrides to the alias at the profile level

```
alias network <NETWORK-ALIAS-NAME> <NETWORK-ADDRESS/MASK>
```

network <NETWORK-ALIAS-NAME>	Creates a new network alias for this profile. Or associates an existing network alias with this profile. A network alias maps a name to a single network address. • <NETWORK-ALIAS-NAME> – Specify the network alias name. Alias name should begin with '$'.
<NETWORK-ADDRESS/MASK>	Associates a single network with this network alias • <NETWORK-ADDRESS/MASK> – Specify the network's address and mask. If using an existing network alias, you can apply overrides to the alias at the profile level.

```
alias network-group <NETWORK-GROUP-ALIAS-NAME> [address-range <STARTING-IP> to
<ENDING-IP> {<STARTING-IP> to <ENDING-IP>}|host <HOST-IP> {<HOST-IP>}|
network <NETWORK-ADDRESS/MASK> {<NETWORK-ADDRESS/MASK>}]
```

network <NETWORK-GROUP-ALIAS-NAME>	Creates a new network-group alias for this profile. Or associates an existing network-group alias with this profile. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name. Alias name should begin with '$'. The network-group aliases are used in ACLs, to define the network-specific components. ACLs using aliases can be used across sites by re-defining the network-group alias elements at the device or profile level. After specifying the name, specify the following: a range of IP addresses, host addresses, or a range of network addresses. If using an existing network-group alias, you can apply overrides to the alias at the profile level.
address-range <STARTING-IP> to <ENDING-IP> {<STARTING-IP> to <ENDING-IP>}	Associates a range of IP addresses with this network-group alias • <STARTING-IP> – Specify the first IP address in the range. • to <ENDING-IP> – Specify the last IP address in the range. • <STARTING-IP> to <ENDING-IP> – Optional. Specifies more than one range of IP addresses. A maximum of eight (8) IP address ranges can be configured.

host <HOST-IP> {<HOST-IP>}	Associates a single or multiple hosts with this network-group alias • <HOST-IP> – Specify the hosts' IP address. • <HOST-IP> – Optional. Specifies more than one host. A maximum of eight (8) hosts can be configured.
network <NETWORK-ADDRESS/MASK> {<NETWORK-ADDRESS/MASK>}	Associates a single or multiple networks with this network-group alias • <NETWORK-ADDRESS/MASK> – Specify the network's address and mask. • <NETWORK-ADDRESS/MASK> – Optional. Specifies more than one network. A maximum of eight (8) networks can be configured.

```
alias network-service <NETWORK-SERVICE-ALIAS-NAME> proto
[<0-254>|<WORD>|eigrp|gre|
igmp|igp|ospf|vrrp]
{(<1-65535>|<WORD>|bgp|dns|ftp|ftp-data|gopher|https|ldap|nntp|
ntp|pop3|proto|sip|smtp|sourceport [<1-65535>|<WORD>]|ssh|telnet|tftp|www)}
```

alias network-service <NETWORK-SERVICE-ALIAS-NAME>	Creates a new network-service alias for this profile. Or associates an existing network-service alias with this profile. A network-service alias maps a name to network services and the corresponding source and destination software ports. • <NETWORK-SERVICE-ALIAS-NAME> – Specify a network-service alias name. Alias name should begin with '$'. The network-service aliases are used in ACLs, to define the service-specific components. ACLs using aliases can be used across sites by re-defining the network-service alias elements at the device or profile level. If using an existing network-service alias, you can apply overrides to the alias at the profile level.
proto [<0-254>| <WORD>|eigrp|gre| igmp|igp|ospf|vrrp]	Use one of the following options to associate an Internet protocol with this network-service alias: • <0-254> – Identifies the protocol by its number. Specify the protocol number from 0 - 254. This is the number by which the protocol is identified in the *Protocol* field of the IPv4 header and the *Next Header* field of IPv6 header. For example, the *User Datagram Protocol's* (UDP) designated number is 17. • <WORD> – Identifies the protocol by its name. Specify the protocol name. • eigrp – Selects *Enhanced Interior Gateway Routing Protocol* (EIGRP). The protocol number 88. • gre – Selects *Generic Routing Encapsulation* (GRE). The protocol number is 47. • igmp – Selects *Internet Group Management Protocol* (IGMP). The protocol number is 2. • igp – Selects *Interior Gateway Protocol* (IGP). The protocol number is 9. • ospf – Selects *Open Shortest Path First* (OSPF). The protocol number is 89. • vrrp – Selects *Virtual Router Redundancy Protocol* (VRRP). The protocol number is 112.

{(<1-65535>|<WORD>|bgp|dns|ftp|ftp-data|gopher|https|ldap|nntp|ntp|pop3|proto|sip|smtp|sourceport [<1-65535>|<WORD>]|ssh|telnet|tftp|www)}	After specifying the protocol, you may configure a destination port for this service. These keywords are recursive and you can configure multiple protocols and associate multiple destination and source ports. • <1-65535> – Optional. Configures a destination port number from 1 - 65535 • <WORD> – Optional. Identifies the destination port by the service name provided. For example, the *secure shell* (SSH) service uses TCP port 22. • bgp – Optional. Configures the default *Border Gateway Protocol* (BGP) services port (179) • dns – Optional. Configures the default *Domain Name System* (DNS) services port (53) • ftp – Optional. Configures the default *File Transfer Protocol* (FTP) control services port (21) • ftp-data – Optional. Configures the default FTP data services port (20) • gopher – Optional. Configures the default gopher services port (70) Contd..

	• https – Optional. Configures the default HTTPS services port (443)
	• ldap – Optional. Configures the default *Lightweight Directory Access Protocol* (LDAP) services port (389)
	• nntp – Optional. Configures the default Newsgroup (NNTP) services port (119)
	• ntp – Optional. Configures the default *Network Time Protocol* (NTP) services port (123)
	• POP3 – Optional. Configures the default *Post Office Protocol* (POP3) services port (110)
	• proto – Optional. Use this option to select another Internet protocol in addition to the one selected in the previous step.
	• sip – Optional. Configures the default *Session Initiation Protocol* (SIP) services port (5060)
	• smtp – Optional. Configures the default *Simple Mail Transfer Protocol* (SMTP) services port (25)
	• sourceport [<1-65535>|<WORD>] – Optional. After specifying the destination port, you may specify a single or range of source ports.
	  • <1-65535> – Specify the source port from 1 - 65535.
	  • <WORD> – Specify the source port range, for example 1-10.
	• ssh – Optional. Configures the default SSH services port (22)
	• telnet – Optional. Configures the default Telnet services port (23)
	• tftp – Optional. Configures the default *Trivial File Transfer Protocol* (TFTP) services port (69)
	• www – Optional. Configures the default HTTP services port (80)

`alias string <STRING-ALIAS-NAME> <LINE>`

alias string <STRING-ALIAS-NAME>	Creates a new string alias for this profile. Or associates an existing string alias with this profile. String aliases map a name to an arbitrary string value. For example, alias string $DOMAIN test.brocade.com'. In this example, the string alias name is: *$DOMAIN* and the string value it is mapped to is: *test.brocade.com*. In this example, the string alias refers to a domain name • <VLAN-ALIAS-NAME> – Specify the string alias name. • <LINE> – Specify the string value. Alias name should begin with '$'. If using an existing string alias, you can apply overrides to the alias at the RF Domain level.

`alias vlan <VLAN-ALIAS-NAME> <1-4094>`

alias vlan <VLAN-ALIAS-NAME>	Creates a new VLAN alias for this profile. Or associates an existing VLAN alias with this profile. A VLAN alias maps a name to a VLAN ID. • <VLAN-ALIAS-NAME> – Specify the VLAN alias name. Alias name should begin with '$'.
<1-4094>	Maps the VLAN alias to a VLAN ID • <1-4094> – Specify the VLAN ID from 1 - 4094. If using an existing VLAN alias, you can apply overrides to the alias at the profile level.

Example

The following example shows the global aliases configured. Note the network-service alias '$kerberos' settings.

```
rfs4000-229D58(config)#show context
!
! Configuration of Brocade Mobility RFS4000 version 5.5.0.0-053B
!
!
version 2.3
!
!
alias network-group $TestNetGrpAlias network 192.168.13.0/24 192.168.16.0/24
alias network-group $TestNetGrpAlias address-range 192.168.13.7 to
192.168.13.16 192.168.13.20 to 192.168.13.25
!
alias network $TestNetworkAlias 192.168.13.0/24
!
alias host $TestHostAlias 192.168.13.10
!
alias address-range $TestAddRanAlias 192.168.13.10 to 192.168.13.13
!
alias network-service $NetworkServAlias proto udp
!
alias network-service $kerberos proto tcp 749 750 80 proto udp 68 sourceport
67
!
alias vlan $TestVLANAlias 1
--More--
rfs4000-229D58(config)#
```

The following examples show the overrides applied to the network-service alias ‘$kerberos’ at the profile level:

```
rfs4000-229D58(config-profile-TestBrocade Mobility RFS4000)#alias
network-service $kerberos proto
 tcp 88 proto udp 80
rfs4000-229D58(config-profile-TestBrocade Mobility RFS4000)#

The following example shows the overrides applied to the network-service alias
‘$kerberos’ at the profile level:
rfs4000-229D58(config-profile-TestBrocade Mobility RFS4000)#show context
profile rfs4000 TestBrocade Mobility RFS4000
 no autoinstall configuration
 no autoinstall firmware
.............................................................
  interface ge5
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface wwan1
 interface pppoe1
 use firewall-policy default
 service pm sys-restart
 router ospf
 alias network-service $kerberos proto tcp 88 proto udp 80
rfs4000-229D58(config-profile-TestBrocade Mobility RFS4000)#
```

Related Commands:

no	Removes the use of centralized auto provisioning policy on this profile or device

area

Profile Config Commands

Sets the system's area of location (the area name)

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
area <WORD>
```

Parameters

```
area <WORD>
```

area <WORD>	Sets the system's area of location • <WORD> – Specify the area name.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#area Ecospace
rfs7000-37FABE(config-profile-default-rfs7000)#

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 bridge vlan 1
  ip igmp snooping
  ip igmp snooping querier
 area Ecospace
 autoinstall configuration
 autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 interface me1
 interface ge1
--More--
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Resets the configured area name

arp

Profile Config Commands

Adds a static *Address Resolution Protocol* (ARP) IP address in the ARP cache

The ARP protocol maps an IP address to a hardware MAC address recognized on the network. ARP provides protocol rules for making this correlation and providing address conversion in both directions.

When an incoming packet destined for a host arrives, ARP finds a physical host or MAC address that matches the IP address. ARP looks in its ARP cache and, if it finds the address, provides it so the packet can be converted to the right packet length, formatted, and sent to its destination. If no entry is found for the IP address, ARP broadcasts a request packet in a special format on the LAN to locate a device that recognizes the IP address. A device that recognizes the IP address as its own returns a reply indicating it. ARP updates the ARP cache for future reference and then sends the packet to the MAC address that replied.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
arp [<IP>|timeout]

arp <IP> <MAC> arpa [<L3-INTERFACE-NAME>|pppoe1|vlan <1-4094>|wwan1|serial
<1-4>
          <1-1> <1-1>] {dhcp-server|router}

arp timeout <15-86400>
```

Parameters

```
arp <IP> <MAC> arpa [<L3-INTERFACE-NAME>|pppoe1|vlan <1-4094>|wwan1|serial
<1-4>
<1-1> <1-1>] {dhcp-server|router}
```

arp <IP>	Adds a static ARP IPv4 address in the ARP cache • <IP> – Specify the static IP address.
<MAC>	Specify the MAC address associated with the IP and the *Switch Virtual Interface* (SVI).
arpa	Sets ARP encapsulation type to ARPA
<L3-INTERFACE-NAME>	Configures static ARP entry for a specified router interface • <L3-INTERFACE-NAME> – Specify the router interface name.
pppoe1	Configures static ARP entry for PPP over Ethernet interface
vlan <1-4094>	Configures static ARP entry for a VLAN interface • <1-4094> – Specify a SVI VLAN ID from 1 - 4094.
wwan1	Configures static ARP entry for Wireless WAN interface

serial <1-4> <1-1> <1-1>	Configures the static ARP entry for serial interface • <1-4> – Specify the Slot ID • <1-1> – Specify the port ID. • <1-1> – Specify the Channel group ID.
{dhcp-server|router}	The following keywords are common to all off the above interface types: • dhcp-server – Optional. Sets ARP entries for a DHCP server • router – Optional. Sets ARP entries for a router

```
arp timeout <15-86400>
```

arp timeout <15-86400>	Sets ARP entry timeout • <TIME> – Sets the ARP entry timeout in seconds. Specify a value from 15 - 86400 seconds.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#arp timeout 2000

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
 arp timeout 2000
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 interface me1
 interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge2
  ip dhcp trust
--More--
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Removes an entry from the ARP cache

auto-learn-staging-config

Profile Config Commands

Enables automatic recognition of devices pending adoption

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — , Brocade Mobility RFS9510

Syntax:

```
auto-learn-staging-config
```

Parameters

None

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#auto-learn-staging-config
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Disables automatic recognition of devices pending adoption

autogen-uniqueid

Profile Config Commands

Autogenerates a unique ID for devices using this profile. When executed in the device configuration mode, this command generates a unique ID for the logged device.

A device's unique ID is a combination of a user-defined string (prefix, suffix, or both) and a substitution token. The Mobility 5.5 implementation provides two built-in substitution tokens: $SN and $MiNT-ID that represent the device's serial number and MiNT-ID respectively. These substitution tokens are internally retrieved and combined with the user-defined string to auto generate a unique identity for a device.

The general format of this command is: <PREFIX><SUBSTITUTION-TOKEN><SUFFIX>. You can provide both (prefix and suffix) or just a prefix or suffix.

For example, given the following set of inputs:

- user-defined prefix – MotoBR1220
- substitution token – $SN

The unique ID is generated using MotoBR1220$SN, where $SN is replaced with the device's serial number.

When executed on an Brocade Mobility 1220 Access Point (having serial number B4C7996C8809), the autogen-uniqueid MotoBR1220$SN command generates the unique ID: Moto*BR1220B4C7996C8809*. When configured on an Brocade Mobility 1220 Access Point profile, all Brocade Mobility 1220 Access Points using the profile autogenerate a unique ID in which the device's serial number is preceded by the string 'MotoBR1220'.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
autogen-uniqueid <WORD>
```

Parameters

```
autogen-uniqueid <WORD>
```

autogen-uniqueid <WORD>	Autogenerates a device's unique ID (not exceeding 64 characters in length) The ID generated is a combination of the text provided and the substitution token $SN or $MiNT-ID. Where ever the autogen-uniqueid is used the device's serial number *OR* MiNT-ID is referenced depending on the substitution token used. • <WORD> – Specify a auto generate unique ID format using one of the following substitution tokens: Available tokens: $SN - references SERIAL NUMBER of the device $MINT-ID - references MINT-ID of the device For example, ORG-$SN-DEPT, In this example 'ORG' and 'DEPT' represent the user-defined prefix and suffix respectively. And $SN is the substitution token.

Example

```
nx4500-5CFA2B(config-profile-testBR6522)#autogen-uniqueid MotoBR6522$SN

nx4500-5CFA2B(config-profile-testBR6522)#show context
autogen-uniqueid MotoBR6522$SN
 no autoinstall configuration
 no autoinstall firmware
 interface radio1
 interface ge1
 use firewall-policy default
 service pm sys-restart
nx4500-5CFA2B(config-profile-testBR6522)#

nx4500-5CFA2B(config-device-B4-C7-99-5C-FA-2B)#autogen-uniqueid
Moto-$MiNT-ID-TechPubs

nx4500-5CFA2B(config-device-B4-C7-99-5C-FA-2B)#show context
nx45xx B4-C7-99-5C-FA-2B
 use profile default-nx45xx
 use rf-domain default
 hostname nx4500-5CFA2B
 license AP DEFAULT-12AP-LICENSE
 license ADSEC DEFAULT-ADV-SEC-LICENSE
 environmental-sensor temperature
 autogen-uniqueid Moto-$MiNT-ID-TechPubs
 ip default-gateway 192.168.13.2
 interface up1
  no shutdown
  switchport mode access
  switchport access vlan 1
 interface vlan1
  ip address 192.168.13.12/24
 logging on
 logging console warnings
 logging buffered warnings
nx4500-5CFA2B(config-device-B4-C7-99-5C-FA-2B)#
```

Related Commands:

no	When executed in the device configuration mode, removes the device's autogen-uniqueid. When executed in the profile configuration mode, removes the autogen-uniqueid on all devices using the profile.

autoinstall

Profile Config Commands

Automatically installs firmware image and configuration parameters on to the selected device.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
autoinstall [configuration|firmware|start-interval <WORD>]
```

Parameters

```
autoinstall [configuration|firmware|start-interval <WORD>]
```

configuration	Autoinstalls startup configuration. Setup parameters are automatically configured on devices using this profile
firmware	Autoinstalls firmware image. Firmware images are automatically installed on devices using this profile
start-interval <WORD>	Configures the interval between system boot and start of autoinstall process (this is the time, from system boot, after which autoinstall should start) • <WORD> – Specify the interval in minutes.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#autoinstall configuration

rfs7000-37FABE(config-profile-default-rfs7000)#autoinstall firmware

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
 arp timeout 2000
 autoinstall configuration
 autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
```

```
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 interface me1
 interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge2
  ip dhcp trust
--More--
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Disables the auto install settings

bridge

Profile Config Commands

The following table summarizes Ethernet bridge configuration commands.

Command	Description	Reference
bridge	Enables Ethernet bridge configuration context	*page 7-557*
bridge-vlan-mode commands	Summarizes bridge VLAN configuration mode commands	page 560

bridge

bridge

Configures VLAN Ethernet bridging parameters. Use this command to configure a Bridge NAT or Bridge VLAN settings.

Configuring bridge *Network Address Translation* (NAT) parameters, allows management of Internet traffic originating at a remote site. In addition to traditional NAT functionality, bridge NAT provides a means of configuring NAT for bridged traffic through an access point. NAT rules are applied to bridged traffic through the access point, and matching packets are NATed to the WAN link instead of being bridged on their way to the router. Using bridge NAT, a tunneled VLAN (extended VLAN) is created between the NoC and a remote location. When a remote client needs to access the Internet, Internet traffic is routed to the NoC, and from there routed to the Internet. This increases the access time for the end user on the client. To resolve latency issues, bridge NAT identifies and segregates traffic heading towards the NoC and outwards towards the Internet. Traffic towards the NoC is allowed over the secure tunnel. Traffic towards the Internet is switched to a local WLAN link with access to the Internet.

A *Virtual LAN* (VLAN) is a separately administrated virtual network within the same physical managed network. VLANs are broadcast domains defined within wireless controllers or service platforms to allow control of broadcast, multicast, unicast, and unknown unicast within a layer 2 device. For example, say several computers are used in conference room X and some in conference Y. The systems in conference room X can communicate with one another, but not with the systems in conference room Y. The VLAN enables the systems in conference rooms X and Y to communicate with one another even though they are on separate physical subnets. The systems in conference rooms X and Y are managed by the same single wireless controller or service platform, but ignore

the systems that are not using the same VLAN ID. Administrators often need to route traffic between different VLANs. Bridging VLANs are only for non-routable traffic, like tagged VLAN frames destined to some other device, which will untag it. When a data frame is received on a port, the VLAN bridge determines the associated VLAN based on the port of reception. Using forwarding database information, the bridge VLAN forwards the data frame on the appropriate port(s). VLANs are useful to set separate networks to isolate some computers from others, without actually having to have separate cabling and Ethernet switches. Controllers can do this on their own, without need for the computer or other gear to know itself what VLAN it is on (this is called port-based VLAN, since it is assigned by port of the switch). Another common use is to put specialized devices like VoIP Phones on a separate network for easier configuration, administration, security, or quality of service.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — , Brocade Mobility RFS9510

NOTE
The interfaces mentioned below are supported as follows:
- ge <index> – Brocade Mobility RFS7000 and Brocade Mobility RFS4000 supports 4 GEs, supports 8 GEs
- me1 – Only supported on Brocade Mobility RFS7000 and Brocade Mobility RFS6000

Syntax:

```
bridge [nat|vlan]

bridge nat source list <IP-ACCESS-LIST-NAME> precedence <1-500> interface
          [<LAYER3-INTERFACE-NAME>|pppoe1|vlan <1-4094>|wwan1]
[(address|interface|overload|
          pool <NAT-POOL-NAME>)]

bridge vlan <1-4095>
```

Parameters

```
bridge nat source list <IP-ACCESS-LIST-NAME> precedence <1-500> interface
[<LAYER3-INTERFACE-NAME>|pppoe1|vlan <1-4094>|wwan1]
[(address|interface|overload|pool <NAT-POOL-NAME>)]
```

nat	Configures bridge NAT parameters
source	Configures NAT source addresses
list <IP-ACCESS-LIST-NAME> precedence <1-500>	Associates an *access control list* (ACL) with this bridge NAT policy. The ACL specifies the IP address permit/deny rules applicable to this bridge NAT policy. • <IP-ACCESS-LIST-NAME> – Specify access list name. • precedence <1-500> – Specifies a precedence value for this bridge NAT policy.

interface [<LAYER3-INTERFACE-NAME>| pppoe1| vlan <1-4094>| wwan1]	Selects one of the following as the primary interface (between the source and destination points): • <LAYER3-INTERFACE-NAME> – A router interface. Specify interface name. • pppoe1 – A PPP over Ethernet interface • vlan <1-4094> – A VLAN interface. Specify the VLAN interface index from 1 - 4094. • wwan1 – A Wireless WAN interface
[(address|interface| overload| pool <NAT-POOL-NAME>)]	The following keywords are recursive and common to all interface types: • address – Configures the interface IP address used for NAT • interface – Configures the failover interface (default setting) • overload – Enables use of one global address for multiple local addresses (terminates command) • pool <NAT-POOLNAME> – Configures the NAT pool used with this bridge NAT policy. Specify the NAT pool name. For more information on configuring a NAT pool, see *nat-pool-config-instance*.

```
bridge vlan <1-4095>
```

vlan <1-4095>	Configures the numerical identifier for the Bridge VLAN when it was initially created. • <1-4095> – Specify a VLAN index from 1 - 4095.

Usage Guidelines:

Creating customized filter schemes for bridged networks limits the amount of unnecessary traffic processed and distributed by the bridging equipment.

If a bridge does not hear *Bridge Protocol Data Units* (BPDUs) from the root bridge within the specified interval, defined in the max-age (seconds) parameter, assume the network has changed and recomputed the spanning-tree topology.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#bridge vlan 1
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#?
Bridge VLAN Mode commands:
  bridging-mode                     Configure how packets on this VLAN are
                                    bridged
  description                       Vlan description
  edge-vlan                         Enable edge-VLAN mode
  firewall                          Enable vlan firewall
  ip                                Internet Protocol (IP)
  l2-tunnel-broadcast-optimization  Enable broadcast optimization
  no                                Negate a command or set its defaults
  stateful-packet-inspection-l2     Enable stateful packet inspection in
                                    layer2 firewall
  tunnel                            Vlan tunneling settings
  tunnel-over-level2                Tunnel extended VLAN traffic over level 2
                                    MiNT links
  use                               Set setting to use

  clrscr                            Clears the display screen
  commit                            Commit all changes made in this session
  do                                Run commands from Exec mode
  end                               End current mode and change to EXEC mode
  exit                              End current mode and down to previous mode
  help                              Description of the interactive help system
  revert                            Revert changes
  service                           Service Commands
  show                              Show running system information
  write                             Write running configuration to memory or
                                    terminal
```

```
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#
```

bridge-vlan-mode commands

bridge

The following table summarizes bridge VLAN configuration mode commands.

Command	Description	Reference
bridging-mode	Configures how packets on this VLAN are bridged	*page 7-560*
description	Configures VLAN bridge description	page 561
edge-vlan	Enables edge VLAN mode	page 562
firewall	Enables VLAN fire wall	*page 7-563*
ip	Configures IP components	page 563
l2-tunnel-broadcast-optimization	Enables broadcast optimization	page 566
no	Negates a command or reverts settings to their default	page 567
stateful-packet-inspection-l2	Enables statedly packet inspection in the layer 2 fire wall	page 569
tunnel	Enables tunneling of unicast messages to unknown MAC destinations, on the selected VLAN bridge	page 570
tunnel-over-level2	Enables extended VLAN traffic over level 2 MiNT links	page 571
use	Uses pre configured access lists with this PF bridge policy	page 572
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug (config-if) instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

bridging-mode

bridge-vlan-mode commands

Configures how packets are bridged on the selected VLAN

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — , Brocade Mobility RFS9510

Syntax:

```
bridging-mode [auto|isolated-tunnel|local|tunnel]
```

Parameters

```
bridging-mode [auto|isolated-tunnel|local|tunnel]
```

bridging-mode	Configures the VLAN bridging modes
auto	Automatically selects the bridging mode to match the WLAN, VLAN and bridging mode configurations (default setting)
isolated-tunnel	Bridges packets between local Ethernet ports and local radios, and passes tunneled packets through without de-tunneling Select this option for a dedicated tunnel for bridging VLAN traffic.
local	Bridges packets normally between local Ethernet ports and local radios (if any) Local mode is typically configured in remote branch offices where traffic on remote private LAN segments need to be bridged locally. Local mode implies that traffic, wired and wireless, are to be bridged locally.
tunnel	Bridges packets between local Ethernet ports, local radios, and tunnels to other APs, wireless controllers, or service platforms Select this option to use a shared tunnel for bridging VLAN traffic. In tunnel mode, the traffic at the AP is always forwarded through the best path. The APs decide the best path to reach the destination and forward packets accordingly. Setting the VLAN to tunnel mode ensures packets are bridged between local Ethernet ports, any local radios, and tunnels to other APs, wireless controllers, and service platforms.

Usage Guidelines:

ACLs can only be used with tunnel or isolated-tunnel modes. They do not work with the local and automatic modes.

Example

```
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#bridging-mode
isolated-tunnel

rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#show context
 bridge vlan 1
 bridging-mode isolated-tunnel
 ip igmp snooping
 ip igmp snooping querier
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#
```

Related Commands:

no	Resets bridging mode to auto

description

bridge-vlan-mode commands

Configures VLAN bridge description

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — , Brocade Mobility RFS9510

Syntax:

```
description <WORD>
```

Parameters

```
description <WORD>
```

description <WORD>	Configures a description for this VLAN bridge • <WORD> – Specify VLAN description. The description should be unique to the VLAN's specific configuration to help differentiate it from other VLANs with similar configurations.

Example

```
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#description
“This is a description for the bridged VLAN”

rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)##show context
 bridge vlan 1
 description This\ is\ a\ description\ for\ the\ bridged\ VLAN
 bridging-mode isolated-tunnel
 ip igmp snooping
 ip igmp snooping querier
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#
```

Related Commands:

no	Removes VLAN bridge description

edge-vlan

bridge-vlan-mode commands

Enables the edge VLAN mode. In the edge VLAN mode, a protected port does not forward traffic to another protected port on the same wireless controller or service platform. This feature enabled by default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — , Brocade Mobility RFS9510

Syntax:

```
edge-vlan
```

Parameters

None

Example

```
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#edge-vlan
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#
```

Related Commands:

no	Disables the edge VLAN mode

firewall

bridge-vlan-mode commands

Enables firewall on this VLAN interface. This feature is enabled by default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
firewall
```

Parameters

None

Example

```
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#firewall
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#
```

Related Commands:

no	Disables a VLAN's firewall

ip

bridge-vlan-mode commands

Configures VLAN bridge IP components

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
ip [arp|dhcp|igmp]
```

```
ip [arp|dhcp] trust

ip igmp snooping {forward-unknown-multicast|mrouter|querier}

ip igmp snooping {forward-unknown-multicast}

ip igmp snooping {mrouter [interface|learn]}
ip igmp snooping {mrouter [interface <INTERFACE-LIST>|learn pim-dvmrp]}

ip igmp {querier} {address|max-response-time|timer|version}
ip igmp snooping {querier} {address <IP>|max-response-time <1-25>|
          timer expiry <60-300>|version <1-3>}
```

Parameters

`ip [arp|dhcp] trust`

ip	Configures the VLAN bridge IP parameters
arp trust	Configures the ARP trust parameter. Trusted ARP packets are used to update the DHCP snoop table to prevent IP spoof and arp-cache poisoning attacks. This option is disabled by default. • trust – Trusts ARP responses on the VLAN bridge
dhcp trust	Configures the DHCP trust parameter. Uses DHCP packets, from a DHCP server, as trusted and permissible within the access point, wireless controller, or service platform managed network. DHCP packets are used to update the DHCP snoop table to prevent IP spoof attacks. This feature is disabled by default. • trust – Trusts DHCP responses on the VLAN bridge

`ip igmp snooping {forward-unknown-multicast}`

ip	Configures the VLAN bridge IP parameters
igmp snooping	Configures Internet *Group Management Protocol* (IGMP) snooping parameter The IGMP protocol establishes and maintains multicast group memberships for interested members. Multicasting allows a networked device to listen to IGMP network traffic and forward IGMP multicast packets to radios on which the interested hosts are connected. The device also maintains a map of the links that require multicast streams, there by reducing unnecessary flooding of the network with multicast traffic.
forward-unknown-multicast	Optional. Enables forwarding of multicast packets from unregistered multicast groups. If disabled, the unknown multicast forward feature is also disabled for individual VLANs. This option is disabled by default.

`ip igmp snooping {mrouter [interface <INTERFACE-LIST>|learn pim-dvmrp]}`

ip	Configures the VLAN bridge IP parameters
igmp snooping	Configures the IGMP snooping parameters
mrouter	Optional. Configures the multicast router parameters
interface <INTERFACE-LIST>	Configures the multicast router interfaces • <INTERFACE-LIST> – Specify a comma-separated list of interface names.
learn pim-dvmrp	Configures the multicast router learning protocols • pim-dvmrp – Enables *Protocol-Independent Multicast* (PIM) and *Distance-Vector Multicast Routing Protocol* (DVMRP) snooping of packets

```
ip igmp snooping {querier} {address <IP>|max-response-time <1-25>|
timer expiry <60-300>|version <1-3>}
```

ip	Configures the VLAN bridge IP parameters
igmp snooping	Configures the IGMP snooping parameters
querier	Optional. Configures the IGMP querier parameters Enables IGMP querier. IGMP snoop querier keeps host memberships alive. It is primarily used in a network where there is a multicast streaming server and hosts subscribed to the server and no IGMP querier present. The access point, wireless controller, or service platform performs the IGMP querier role. An IGMP querier sends out periodic IGMP query packets. Interested hosts reply with an IGMP report packet. IGMP snooping is only conducted on wireless radios. IGMP multicast packets are flooded on wired ports. IGMP multicast packet are not flooded on the wired port. IGMP membership is also learnt on it and only if present, then it is forwarded on that port.
address <IP>	Optional. Configures the IGMP querier source IP address • <IP> – Specify the IGMP querier source IP address.
max-response-time <1-25>	Optional. Configures the IGMP querier maximum response time • <1-25> – Specify the maximum response time from 1 - 25 seconds. The default is 10 seconds. The access point, wireless controller, or service platform forwards multicast packets only to radios present in the snooping table. IGMP reports from wired ports are forwarded to the multicast router ports. If no reports are received from a radio, it is removed from the snooping table. The radio then stops receiving multicast packets.
timer expiry <60-300>	Optional. Configures the IGMP querier timeout • expiry – Configures the IGMP querier timeout • <60-300> – Specify the IGMP querier timeout from 60 - 300 seconds.
version <1-3>	Optional. Configures the IGMP version • <1-3> – Specify the IGMP version. The versions are 1- 3. The default is 3.

Example

```
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#ip arp trust

rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#ip dhcp trust

rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#ip igmp snooping
mrouter interface ge1 ge2

rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#ip igmp snooping
mrouter learn pim-dvmrp

rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#ip igmp snooping
querier max-response-time 24

rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#ip igmp snooping
querier timer expiry 100

rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#ip igmp snooping
querier version 2

rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#show context
bridge vlan 1
  description This\ is\ a\ description\ of\ the\ bridged\ VLAN
  ip arp trust
  ip dhcp trust
  ip igmp snooping
  ip igmp snooping querier
  ip igmp snooping querier version 2
```

```
  ip igmp snooping querier max-response-time 24
  ip igmp snooping querier timer expiry 100
  ip igmp snooping mrouter interface ge2 ge1
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#
```

Related Commands:

no	Disables or reverts the VLAN Ethernet bridge parameters

l2-tunnel-broadcast-optimization

bridge-vlan-mode commands

Enables broadcast optimization on this VLAN interface. Enabling this feature aids in the identification of each incoming packet. This feature is disabled by default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
l2-tunn2l-broadcast-optimization
```

Parameters

None

Example

```
rfs7000-37FABE(config-profile
default-rfs7000-bridge-vlan-1)#l2-tunnel-broadcast
-optimization

rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#show context
 bridge vlan 1
  description This\ is\ a\ description\ for\ the\ bridged\ VLAN
  l2-tunnel-broadcast-optimization
  bridging-mode isolated-tunnel
  ip arp trust
  ip dhcp trust
  ip igmp snooping
  ip igmp snooping querier
  ip igmp snooping mrouter interface ge2 ge1
  ip igmp snooping querier version 2
  ip igmp snooping querier max-response-time 24
  ip igmp snooping querier timer expiry 100
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#
```

Related Commands:

no	Disables broadcast optimization

no

bridge-vlan-mode commands

Negates a command or reverts settings to their default. The no command, when used in the bridge VLAN mode, negates the VLAN bridge settings or reverts them to their default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no
[bridging-mode|description|edge-vlan|firewall|ip|l2-tunnel-broadcast-optimiza
tion|
          stateful-packet-inspection-l2|tunnel|tunnel-over-level2|use]

no
[bridging-mode|description|edge-vlan|firewall|l2-tunnel-broadcast-optimizatio
n|
          stateful-packet-inspection-l2|tunnel-over-level12]

no ip [arp|dhcp|igmp]

no ip [arp|dhcp] trust
no ip igmp snooping {forward-unknown-multicast|mrouter|querier}
no ip igmp snooping {forward-unknown-multicast}
no ip igmp snooping {mrouter [interface <INTERFACE-LIST>|learn pin-dvmrp]}
no ip igmp snooping {querier {address|max-response-time|timer expiry|version}}

no tunnel unknown-unicast

no use [ip-access-list|mac-access-list] tunnel out
```

Parameters

```
no
[bridging-mode|description|edge-vlan|firewall|l2-tunnel-broadcast-optimizatio
n|
stateful-packet-inspection-12|tunnel-over-level2]
```

no bridging-mode	Resets the bridging mode to ‘auto’
no description	Removes the VLAN’s description
no edge-vlan	Disables the edge VLAN mode
no firewall	Disables the VLAN’s firewall
no l2-tunnel-broadcast-optimization	Disables broadcast optimization

no tunnel-over-level~~1~~2	Disables extended VLAN traffic over level 2 MiNT links
no stateful-packet-inspection-12	Disables stateful packet inspection in the layer 2 firewall

no ip [arp|dhcp] trust

no ip	Negates or reverts VLAN bridge IP settings
arp trust	Disables the trust of ARP responses on the VLAN
dhcp trust	Disables the trust of DHCP responses on the VLAN

no ip igmp snooping *{forward-unknown-multicast}*

no ip	Negates or reverts the VLAN bridge IP settings
igmp snooping	Negates or reverts the IGMP snooping settings
forward-unknown-multicast	Optional. Disables the forwarding of unknown multicast packets

no ip igmp snooping *{mrouter [interface <INTERFACE-LIST>|learn pim-dvmrp]}*

no ip	Negates or reverts the VLAN bridge IP settings
igmp snooping	Negates or reverts the IGMP snooping settings
mrouter	Optional. Resets or disables multicast router parameters
interface <INTERFACE-LIST>	Optional. Disables mrouter interfaces • <INTERFACE-LIST> – Specify a list of interface names separated by a space.
learn pim-dvmrp	Optional. Disables multicast router learning protocols • pim-dvmrp – Disables PIM-DVMRP snooping of packets

no ip igmp snooping *{querier {address|max-response-time|timer expiry|version}}*

no ip	Negates or reverts the VLAN bridge IP settings
igmp snooping	Negates the IGMP snooping components
querier	Optional. Disables the IGMP querier
address	Optional. Reverts to the default IGMP querier source IP address of 0.0.0.0
max-response-time	Optional. Reverts to the default IGMP querier maximum response time
timer expiry	Optional. Reverts to the default IGMP querier timeout
version <1-3>	Optional. Reverts to the default IGMP version

no tunnel unknown-unicast

no tunnel unknown-unicast	Disables tunneling of unicast messages, to unknown MAC destinations, on the selected VLAN bridge

no use [br-access-list|mac-access-list] tunnel out

no use	Removes the VLAN bridge's IP access list or MAC access list
ip-access-list tunnel out	Removes the VLAN bridge's IP access list • tunnel – Prevents the IP access list from being applied to all packets going into a tunnel • out – Prevents the IP access list from being applied to all outgoing packets
mac-access-list tunnel out	Removes the VLAN bridge's MAC access list • tunnel – Prevents the MAC access list from being applied to all packets going into a tunnel • out – Prevents the MAC access list from being applied to all outgoing packets

Example

```
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#no description
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#no ip igmp
snooping mrouter interface ge1
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#no ip igmp
snooping mrouter learn pim-dvmrp
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#no ip igmp
snooping querier max-response-time
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#no ip igmp
snooping querier version

rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#show context
 bridge vlan 1
  no edge-vlan
  no stateful-packet-inspection-l2
  ip igmp snooping
  no ip igmp snooping unknown-multicast-fwd
  no ip igmp snooping mrouter learn pim-dvmrp
  no ip igmp snooping querier
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#
```

Related Commands:

bridging-mode	Configures the VLAN's bridging mode
description	Configures the VLAN's description
edge-vlan	Enables the edge VLAN mode
ip	Configures the VLAN's IP components
l2-tunnel-broadcast-optimization	Enables broadcast optimization
stateful-packet-inspection-l2	Enables stateful packet inspection in the layer 2 firewall
tunnel	Enables tunneling of unicast messages to unknown MAC destinations, on the selected VLAN bridge
tunnel-over-level2	Enables extended VLAN traffic over level 2 MiNT links
use	Uses pre configured access lists with this PF bridge policy
clrscr	Clears the display screen
commit	Commits (saves) changes made in the current session
end	Ends and exits the current mode and moves to the PRIV EXEC mode
exit	Ends the current mode and moves to the previous mode
help	Displays interactive help system
revert	Reverts changes to their last saved configuration
service	Invokes service commands to troubleshoot or debug (config-if) instance configurations
show	Displays running system information
write	Writes information to memory or terminal

stateful-packet-inspection-l2

bridge-vlan-mode commands

Enables a stateful packet inspection at the layer 2 firewall

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
stateful-packet-inspection-l2
```

Parameters

None

Example

```
rfs7000-37FABE(config-profile
default-rfs7000-bridge-vlan-1)#stateful-packet-ins
inspection-l2
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#
```

Related Commands:

no	Disables stateful packet inspection at the layer 2 firewall

tunnel

bridge-vlan-mode commands

Enables tunneling of unicast messages, to unknown MAC destinations, on the selected VLAN bridge

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
tunnel unknown-unicast
```

Parameters

None

Example

```
rfs7000-37FABE(config-profile TestAP81xx-bridge-vlan-1)#tunnel
unknown-unicast
rfs7000-37FABE(config-profile TestAP81xx-bridge-vlan-1)#
```

```
rfs7000-37FABE(config-profile TestAP81xx-bridge-vlan-1)#no tunnel
unknown-unicast

rfs7000-37FABE(config-profile TestAP81xx-bridge-vlan-1)#show context
 bridge vlan 1
  ip igmp snooping
  ip igmp snooping querier
  no tunnel unknown-unicast
rfs7000-37FABE(config-profile TestAP81xx-bridge-vlan-1)#
```

Related Commands:

no	Disables tunneling of unicast messages, to unknown MAC destinations, on the selected VLAN bridge

tunnel-over-level2

bridge-vlan-mode commands

Enables extended VLAN (tunneled VLAN) traffic over level 2 MiNT links

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
tunnel-over-level2
```

Parameters

None

Example

```
rfs4000-229D58(config-profile testBrocade Mobility
RFS4000-bridge-vlan-1)#tunnel-over-level2
rfs4000-229D58(config-profile testBrocade Mobility
RFS4000-bridge-vlan-1)#commit

rfs4000-229D58(config-profile testBrocade Mobility
RFS4000-bridge-vlan-1)#show context
 bridge vlan 1
  description This\ is\ a\ test\ bridge\ VLAN
  l2-tunnel-broadcast-optimization
  bridging-mode isolated-tunnel
  tunnel-over-level2
  ip arp trust
  ip dhcp trust
  ip igmp snooping
  ip igmp snooping querier
rfs4000-229D58(config-profile testBrocade Mobility RFS4000-bridge-vlan-1)#
```

Related Commands:

no	Disables extended VLAN traffic over level 2 MiNT links

use

bridge-vlan-mode commands

Uses pre configured access lists with this bridge policy

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
use [ip-access-list|mac-access-list] tunnel out <IP/MAC-ACCESS-LIST-NAME>
```

Parameters

```
use [ip-access-list|mac-access-list] tunnel out <IP/MAC-ACCESS-LIST-NAME>
```

use	Sets this VLAN bridge policy to use an IP access list or a MAC access list
ip-access-list tunnel	Associates a pre-configured IP access list with this VLAN-bridge interface
mac-access-list	Uses a pre-configured MAC access list with this VLAN- bridge interface
tunnel out <IP/MAC-ACCESS-LIST-NAME>	The following keywords are common to the 'IP access list' and 'MAC access list' parameters: • tunnel – Applies IP access list or MAC access list to all packets going into the tunnel • out – Applies IP access list or MAC access list to all outgoing packets • <IP/MAC-ACCESS-LIST-NAME> – Specify the IP access list or MAC access list name.

Example

```
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#use
mac-access-list tunnel out PERMIT-ARP-AND-IPv4

rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#show context
 bridge vlan 1
  ip igmp snooping
  ip igmp snooping querier
  use mac-access-list tunnel out PERMIT-ARP-AND-IPv4
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#
```

Related Commands:

no	Disables or reverts VLAN Ethernet bridge settings

captive-portal

Profile Config Commands

Configures captive portal advanced Web page uploads on this profile. These Web pages are uploaded to access points supporting the captive portal.

A captive portal is a means of providing guests temporary and restrictive access to the controller managed wireless network. A captive portal provides secure authenticated controller access by capturing and re-directing a wireless user's Web browser session to a captive portal login page, where the user must enter valid credentials. Once the user is authenticated and logged into the controller managed network, additional agreement, welcome, and fail pages provide the administrator with options to control the captive portal's screen flow and user appearance.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
captive-portal page-upload count <1-20>
```

Parameters

```
captive-portal page-upload count <1-20>
```

page-upload	Enables captive portal advanced Web page upload
count <1-20>	Sets the maximum number of APs that can be uploaded concurrently • <1-20> – Set a value from 1 - 20.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#captive-portal page-upload
count 10
rfs7000-37FABE(config-profile-default-rfs7000)#
```

cdp

Profile Config Commands

Uses *Cisco Discovery Protocol* (CDP) as a layer 2 protocol that discovers information about neighboring network devices

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
cdp [holdtime|run|timer]
```

```
cdp [holdtime <10-1800>|run|timer <5-900>]
```

Parameters

```
cdp [holdtime <10-1800>|run|timer <5-900>]
```

holdtime <10-1800>	Specifies the holdtime after which transmitted packets are discarded • <10-1800> – Specify a value from 10 - 1800 seconds. The default is 180 seconds.
run	Enables/disables CDP sniffing and transmit globally. This feature is enabled by default.
timer <5-900>	Specifies time between advertisements • <5-900> – Specify a value from 5 - 900 seconds. The default is 60 seconds.

Example

```
rfs7000-37FABE(config profile-default-rfs7000)#cdp run

rfs7000-37FABE(config profile-default-rfs7000)#cdp holdtime 1000

rfs7000-37FABE(config profile-default-rfs7000)#cdp timer 900

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 bridge vlan 1
  no edge-vlan
  l2-tunnel-broadcast-optimization
 ..........................................................
  qos trust 802.1p
 interface pppoe1
 use firewall-policy default
 cdp holdtime 1000
 cdp timer 900
 service pm sys-restart
 router ospf
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Disables CDP on this profile

cluster

Profile Config Commands

Sets the cluster configuration

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
cluster [force-configured-state|force-configured-state-delay|handle-stp|
          master-priority|member|mode|name]

cluster [force-configured-state|force-configured-state-delay
<3-1800>|handle-stp|
          master-priority <1-255>]

cluster member [ip|vlan]
cluster member [ip <IP> {level [1|2]}|vlan <1-4094>]

cluster mode [active|standby]

cluster name <CLUSTER-NAME>
```

Parameters

```
cluster [force-configured-state|force-configured-state-delay
<3-1800>|handle-stp|
master-priority <1-255>]
```

force-configured-state	Forces adopted APs to auto revert when a failed wireless controller or service platform (in a cluster) restarts When an active controller (wireless controller, or service platform) fails, a standby controller in the cluster takes over APs adopted by the failed active controller. If the failed active controller were to restart, it starts a timer based on the 'force-configured-state-delay' interval specified. At the expiration of this interval, the standby controller releases all adopted APs and goes back to a monitoring mode. If the active controller fails during this interval, the 'force-configured-state-delay' timer is stopped. The timer restarts as soon as the active controller comes back up. This feature is disabled by default.
force-configured-state-delay <3-1800>	Forces cluster transition to the configured state after a specified interval • <3-1800> – Specify a delay from 3 - 1800 minutes. The default is 5 minutes. This is the interval a standby controller waits before releasing adopted APs, when a failed active controller becomes active again.
handle-stp	Enables/disables *Spanning Tree Protocol* (STP) convergence handling. This feature is disabled by default. In layer 2 networks, this protocol is enabled to prevent network looping. If enabled, the network forwards data only after STP convergence. Enabling STP convergence delays the redundancy state machine execution until the STP convergence is completed (the standard protocol value for STP convergence is 50 seconds). Delaying the state machine is important to load balance APs at startup.
master-priority <1-255>	Configures cluster master priority • <1-255> – Specifies cluster master election priority. Assign a value from 1 - 255. Higher the value higher is the precedence. The default is 128. In a cluster environment, one device from the cluster is elected as the cluster master. A device's master priority value decides the device's priority to become cluster master.

```
cluster member [ip <IP> {level [1|2]}|vlan <1-4094>]
```

member	Adds a member to the cluster. It also configures the cluster VLAN where members can be reached.
ip <IP> level [1|2]	Adds IP address of the new cluster member • <IP> – Specify the IP address. • level – Optional. Configures routing level for the new member. Select one of the following routing levels: • 1 – Level 1, local routing • 2 – Level 2, In-site routing
vlan <1-4094>	Configures the cluster VLAN where members can be reached • <1-4094> – Specify the VLAN ID from 1- 4094.

```
cluster mode [active|standby]
```

mode [active|standby]	Configures cluster member's mode as active or standby • active – Configures cluster mode as active. This is the default setting. • standby – Configures cluster mode as standby A member can be in either an Active or Standby mode. All active member controllers can adopt access points. Standby members only adopt access points when an active member has failed or sees an access point not adopted by a controller.

```
cluster name <CLUSTER-NAME>
```

name <CLUSTER-NAME>	Configures the cluster name • <CLUSTER-NAME> – Specify the cluster name.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#cluster name cluster1

rfs7000-37FABE(config-profile-default-rfs7000)#cluster member ip 172.16.10.3

rfs7000-37FABE(config-profile-default-rfs7000)#cluster mode active

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 bridge vlan 1
  description Vlan1
.........................................
 cluster name cluster1
 cluster member ip 172.16.10.3
 cluster member vlan 1
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Removes cluster member

configuration-persistence

Profile Config Commands

Enables configuration persistence across reloads

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
configuration-persistence {secure}
```

Parameters

```
configuration-persistence {secure}
```

secure	Optional. Ensures parts of a file that contain security information are not written during a reload

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#configuration-persistence
secure

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 bridge vlan 1
  no edge-vlan
  ip igmp snooping
  no ip igmp snooping unknown-multicast-fwd
  no ip igmp snooping mrouter learn pim-dvmrp
  autoinstall configuration
 autoinstall firmware
 ..........................................................................
 cluster name cluster1
 cluster member ip 1.2.3.4 level 2
 cluster member ip 172.16.10.3
 cluster member vlan 4094
 cluster handle-stp
 cluster force-configured-state
  holdtime 1000
  timer 900
 configuration-persistence secure
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Disables automatic write up of startup configuration file

controller

Profile Config Commands

Configures the WLAN's controller (wireless controller or service platform) settings

Use this command to add a controller to a pool and group. This command also enables and disables adoption on controllers, and specifies the device types that can be adopted by a controller.

In an *hierarchically managed* (HM) network, devices (controllers and access points) are deployed across three levels. This results in devices that are either adoptee or adopters. For more information on HM network, see *device-upgrade*.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
controller [adopted-devices|adoption|group|hello-interval|vlan|host]

controller adopted-devices [aps|controllers]
controller adopted-devices [aps {controllers}|controllers {aps}]

controller adoption

controller [group <CONTROLLER-GROUP-NAME>|vlan <1-4094>]

controller hello-interval <1-120> adjacency-hold-time <2-600>

controller host [<IP>|<HOSTNAME>] {ipsec-secure|level|pool|remote-vpn-client}
controller host [<IP>|<HOSTNAME>] {level [1|2]|pool <1-2> level [1|2]}
          {(ipsec-secure {gw})}
controller host [<IP>|<HOSTNAME>] {remote-vpn-client}
```

Parameters

`controller adopted-devices [aps {controllers}|controllers {aps}]`

controller	Configures the WLAN's controller settings
adopted-devices	Configures the types of device (AP/controller) this controller can adopt
aps {controllers}	Enables the adoption of access points by this controller. This is the default setting. • controllers – Optional. Enables the adoption of controllers by this controller All adopted devices (referred to as adoptee) receive complete configuration from the adopting controller (referred to as adopter).
controllers {aps}	Enables the adoption of controllers by this controllers • aps – Optional. Enables the adoption of access points by this controller A controller cannot be configured as an adoptee and an adopter simultaneously. In other words, an adopted controller (adoptee) cannot be configured to adopt another controller. Use the *no* > *controller* > *adopted-devices* command to remove this setting.

`controller adoption`

controller adoption	Enables adoption of the logged wireless controller or service platform Use the *no* > *controller* > *adoption* command to disable adoption.

`controller [group <CONTROLLER-GROUP-NAME>|vlan <1-4094>]`

controller	Configures the WLAN's controller settings
group <CONTROLLER-GROUP-NAME>	Configures the wireless controller or service platform group • <CONTROLLER-GROUP-NAME> – Specify the wireless controller or service platform group name.
vlan <1-4094>	Configures the wireless controller or service platform VLAN • <1-4094> – Specify the VLAN ID from 1 - 4094.

`controller hello-interval <1-120> adjacency-hold-time <2-600>`

controller	Configures the WLAN's controller settings
hello-interval <1-120>	Configures the hello-interval in seconds. This is the interval between consecutive hello packets exchanged between AP and wireless controller or service platform. • <1-120> – Specify a value from 1 - 120 seconds.
adjacency-hold-time <2-600>	Configures the adjacency hold time in seconds. This is the time since the last received hello packet, after which the adjacency between wireless controller or service platform and AP is lost, and the link is re-established. • <2-600> – Specify a value from 2 - 600 seconds.

```
controller host [<IP>|<HOSTNAME>] {level [1|2]|pool <1-2> level [1|2]}
{(ipsec-secure {gw})}
```

controller	Configures the WLAN's controller settings
host [<IP>|<HOSTNAME>]	Configures wireless controller or service platform's IP address or name • <IP> – Configures wireless controller or service platform's IP address • <HOSTNAME> – Configures wireless controller or service platform's name
level [1|2]	The following keywords are common to the 'IP' and 'hostname' parameters: Optional. After providing the wireless controller or service platform's address, optionally select one of the following routing levels: • 1 – Optional. Level 1, local routing • 2 – Optional. Level 2, inter-site routing

pool <1-2> level [1|2]	The following keywords are common to the 'IP' and 'hostname' parameters:
	Optional. Sets the wireless controller or service platform's pool
	• <1-2> – Select either 1 or 2 as the pool. The default is 1. After selecting the pool, optionally select one of the following two routing levels:
	  • 1 – Optional. Level 1, local routing
	  • 2 – Optional. Level 2, inter-site routing

ipsec-secure {gw}	The following keywords are recursive and common to the 'level' and 'pool' parameters: • ipsec-secure – Optional. Configures secure gateway with the IPSec tunnel • gw – Optional. Specifies a IPSec gateway other than the wireless controller or service platform

```
controller host [<IP>|<HOSTNAME>] {remote-vpn-client}
```

controller	Configures the WLAN's controller settings
host [<IP>|<HOSTNAME>]	Configures wireless controller or service platform's IP address or name • <IP> – Configures wireless controller or service platform's IP address • <HOSTNAME> – Configures wireless controller or service platform's name
remote-vpn-client	Forces *MiNT link creation protocol* (MLCP) to use remote VPN connection on the controller The controller uses remote VPN tunnel for this traffic. If multiple controller hosts are configured, either all the hosts should use remote-vpn-client or none. When enabled, an MLCP connection is not initiated until remote VPN connection is UP and virtual IP, DNS server, source route etc. are installed on the AP.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#controller group test

rfs7000-37FABE(config-profile-default-rfs7000)#controller host 1.2.3.4 pool 2

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 no autoinstall configuration
 no autoinstall firmware
 crypto isakmp policy default
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 interface me1
 interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge2
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge3
```

```
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge4
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 use firewall-policy default
 controller host 1.2.3.4 pool 2
 controller group test
 service pm sys-restart

rfs4000-229D58(config-profile-testBrocade Mobility RFS4000)#controller
adopted-devices aps controllers

rfs4000-229D58(config-profile-testBrocade Mobility RFS4000)#show context
profile rfs4000 testBrocade Mobility RFS4000
 autoinstall configuration
.................................................................
  logging on
 service pm sys-restart
 router ospf
 controller adopted-devices aps controllers
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000)#
```

Related Commands:

no	Disables or reverts settings to their default

critical-resource

Profile Config Commands

Monitors resources that are critical to the health of the service platform, wireless controller, or access point managed network. These critical resources are identified by their configured IP addresses. When enabled, the system monitors these devices regularly and logs their status.

A critical resource can be a gateway, AAA server, WAN interface, any hardware, or a service on which the stability of the network depends. Monitoring these resources is therefore essential. When enabled, this feature pings critical resources regularly to ascertain their status. If there is a connectivity issue, an event is generated stating a critical resource is unavailable. By default, there is no enabled critical resource policy and one needs to be created and implemented.

Critical resources can be monitored directly through the interfaces on which they are discovered. For example, a critical resource on the same subnet as an Brocade Mobility 1240 Access Point access point can be monitored by its IP address. However, a critical resource located on a VLAN must continue to be monitored on that VLAN.

Critical resource monitoring can be enabled on service platforms, wireless controllers, and access points through their respective device profiles.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
critical-resource [<CRITICAL-RESRC-NAME>|monitor]

critical-resource <CRITICAL-RESRC-NAME> monitor [direct|via]
critical-resource <CRITICAL-RESRC-NAME> monitor direct [all|any] <IP> {<IP>|
          arp-only vlan <1-4094> {<IP>|port [<LAYER2-IF-NAME>|ge
<1-4>|port-channel <1-2>]}}

critical-resource <CRITICAL-RESRC-NAME> monitor via
[<IP>|<LAYER3-INTERFACE-NAME>|
          pppoe1|vlan|wwan1]
critical-resource <CRITICAL-RESRC-NAME> monitor via
[<IP>|<LAYER3-INTERFACE-NAME>|
          pppoe1|vlan <1-4094>|wwan1] [all|any] <IP> {<IP>|arp-only vlan
<1-4094>
          {<IP>|port [<LAYER2-IF-NAME>|ge <1-4>|port-channel <1-2>]}}

critical-resource monitor interval <5-86400>
```

Parameters

```
critical-resource <CRITICAL-RESRC-NAME> monitor direct [all|any] <IP> {<IP>|
arp-only vlan <1-4094> {<IP>|port [<LAYER2-IF-NAME>|ge <1-4>|port-channel
<1-2>]}}
```

<CRITICAL-RESRC-NAME>	Specify the critical resource name
monitor	Monitors configured critical resource(s)
direct [all|any]	Monitors critical resources using the default routing engine • all – Monitors all resources that are going down (generates an event when all specified critical resources are unreachable) • any – Monitors any resource that is going down (generates an event when any one of the specified critical resource is unreachable)
<IP>	Specifies the IP address to monitor
arp-only vlan <1-4094> {<IP>| port [<LAYER2-IFNAME>| ge|port-channel]}	The following keywords are common to the 'all' and 'any' parameters: • arp-only vlan <1-4094> – Optional. Uses ARP to determine if the IP address is reachable (use this option to monitor resources that do not have IP addresses). ARP is used to resolve hardware addresses when only the network layer address is known. • vlan <1-4094> – Specifies the VLAN ID on which to send the probing ARP requests. Specify the VLAN ID from 1 - 4094. • <IP> – Optional. Limits ARP to a device specified by the <IP> parameter • port [<LAYER2-IF-NAME>|ge|port-channel] – Optional. Limits ARP to a specified port

```
critical-resource <CRITICAL-RESRC-NAME> monitor via
[<IP>|<LAYER3-INTERFACE-NAME>|
pppoe1|vlan <1-4094>|wwan1] [all|any] <IP> {<IP>|arp-only [vlan <1-4094>]
{<IP>}}
```

<CRITICAL-RESRC-NAME>	Specify the critical resource name
monitor	Monitors configured critical resource(s)
via	Specifies the interface or next-hop via which the ICMP pings should be sent. Configures the interface or next-hop via which ICMP pings are sent. This does not apply to IP addresses configured for arp-only. For interfaces which learn the default-gateway dynamically (like DHCP clients and PPP interfaces), use an interface name for VIA, or use an IP address.
<IP>	Specify the IP address of the next-hop via which the critical resource(s) are monitored. Configures up to four IP addresses for monitoring. All the four IP addresses constitute critical resources.
<LAYER3-INTERFACE-NAME>	Specify the layer 3 Interface name (router interface)
pppoe1	Specifies PPP over Ethernet interface
vlan <1-4094>	Specifies the wireless controller or service platform's VLAN interface. Specify VLAN ID from 1 - 4094.
wwan1	Specifies Wireless WAN interface
[all|any]	Monitors critical resources using the default routing engine • all – Monitors all resources that are going down (generates an event when all specified critical resource IP addresses are unreachable) • any – Monitors any resource that is going down (generates an event when any one of the specified critical resource IP address is unreachable)
arp-only vlan <1-4094> {<IP>| port [<LAYER2-IFNAME>| ge|port-channel]}	The following keywords are common to the 'all' and 'any' parameters: • arp-only vlan <1-4094> – Optional. Uses ARP to determine if the IP address is reachable (use this option to monitor resources that do not have IP addresses). ARP is used to resolve hardware addresses when only the network layer address is known. • vlan <1-4094> – Specifies the VLAN ID to send the probing ARP requests. Specify the VLAN ID from 1 - 4094. • <IP> – Optional. Limits ARP to a device specified by the <IP> parameter • port [<LAYER2-IF-NAME>|ge|port-channel] – Optional. Limits ARP to a specified port

```
critical-resource monitor interval <5-86400>
```

monitor interval <5-86400>	Configures the critical resource monitoring frequency • <5-86400> – Specifies the frequency in seconds. Specify the time from 5 - 86400 seconds. The default is 30 seconds.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#critical-resource monitor
interval 40

rfs7000-37FABE(config-profile-default-rfs7000)#critical-resource monitor
direct all 172.16.10.2 arp-only vlan 1

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 bridge vlan 1
  bridging-mode isolated-tunnel
  ..................................................
 use firewall-policy default
critical-resource monitor interval 40
 --More--
rfs7000-37FABE(config-profile-default-rfs7000)#
```

crypto

Profile Config Commands

Use the crypto command to define a system-level local ID for *Internet Security Association and Key Management Protocol* (ISAKMP) negotiation and to enter the ISAKMP policy, ISAKMP client, or ISAKMP peer command set.

The following table summarizes crypto configuration commands.

Command	Description	Reference
crypto	Invokes commands used to configure ISAKMP policy, iSAKMP client, and ISAKMP peer	*page 7-583*
crypto-auto-ipsec-tunnel commands	Creates an auto IPSec VPN tunnel and changes the mode to auto-ipsec-secure mode for further configuration	page 588
crypto-ikev1/ikev2-policy commands	Configures crypto IKEv1/IKEv2 policy parameters	page 595
crypto-ikev1/ikev2-peer commands	Configures IKEv1 peer parameters	page 601
crypto-map-config-commands	Configures crypto map parameters	page 607
crypto-remote-vpn-client commands	Configures remote VPN client settings	page 627

crypto

crypto

Use the crypto command to define a system-level local ID for ISAKMP negotiation and enter the ISAKMP policy, ISAKMP client, or ISAKMP peer configuration mode.

A crypto map entry is a single policy that describes how certain traffic is secured. There are two types of crypto map entries: ipsec-manual and ipsec-ike entries. Each entry is given an index (used to sort the ordered list).

When a non-secured packet arrives on an interface, the crypto map associated with that interface is processed (in order). If a crypto map entry matches the non-secured traffic, the traffic is discarded.

When a packet is transmitted on an interface, the crypto map associated with that interface is processed. The first crypto map entry that matches the packet is used to secure the packet. If a suitable SA exists, it is used for transmission. Otherwise, IKE is used to establish a SA with the peer. If no SA exists (and the crypto map entry is “respond only”), the packet is discarded.

When a secured packet arrives on an interface, its *Security Parameter Index* (SPI) is used to look up a SA. If a SA does not exist (or if the packet fails any of the security checks), it is discarded. If all checks pass, the packet is forwarded normally.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
crypto [auto-ipsec-secure|enable-ike-uniqueids|ike-version|ikev1|ikev2|ipsec|

load-management|map|pki|plain-text-deny-acl-scope|remote-vpn-client]

crypto [auto-ipsec-secure|enable-ike-uniqueids|load-management]

crypto ike-version [ikev1-only|ikev2-only]

crypto ikev1 [dpd-keepalive <10-3600>|dpd-retries <1-100>|nat-keepalive
<10-3600>|
          peer <IKEV1-PEER>|policy <IKEV1-POLICY-NAME>|remote-vpn]

crypto ikev2 [cookie-challenge-threshold <1-100>|dpd-keepalive <10-3600>|
          dpd-retries <1-100>|nat-keepalive <10-3600>|peer <IKEV2-PEER>|
          policy <IKEV2-POLICY-NAME>|remote-vpn]

crypto ipsec [df-bit|security-association|transform-set]
crypto ipsec df-bit [clear|copy|set]
crypto ipsec security-association lifetime [kilobytes <500-2147483646>|
          seconds <120-86400>]
crypto ipsec transform-set <TRANSFORM-SET-TAG> [esp-3des|esp-aes|esp-aes-192|
          esp-aes-256|esp-des|esp-null] [esp-md5-hmac|esp-sha-hmac]

crypto map <CRYPTO-MAP-TAG> <1-1000> [ipsec-isakmp {dynamic}|ipsec-manual]

crypto pki import crl <TRUSTPOINT-NAME> URL <1-168>

crypto plain-text-deny-acl-scope [global|interface]

crypto remote-vpn-client
```

Parameters

```
crypto [auto-ipsec-secure|enable-ike-uniqueids|load-management]
```

auto-ipsec-secure	Configures the Auto IPSec Secure parameter settings. For Auto IPSec tunnel configuration commands, see *crypto-auto-ipsec-tunnel commands*.
enable-ike-uniqueids	Enables *Internet Key Exchange* (IKE) unique ID check For more information on IKE unique IDs, see *remotegw*.
load-management	Configures load management for platforms using software cryptography

```
crypto ike-version [ikev1-only|ikev2-only]
```

ike-version [ikev1-only|ikev2-only]	Selects and starts the IKE daemon • ikev1-only – Enables support for IKEv1 tunnels only • ikev2-only – Enables support for IKEv2 tunnels only

```
crypto ikev1 [dpd-keepalive <10-3600>|dpd-retries <1-100>|nat-keepalive
<10-3600>|
peer <IKEV1-PEER>|policy <IKEV1-POLICY-NAME>|remote-vpn]
```

ikev1	Configures the IKEv1 parameters
dpd-keepalive <10-3600>	Sets the global *Dead Peer Detection* (DPD) interval from 10 - 3600 seconds
dpd-retries <1-1000>	Sets the global DPD retries count from 1- 1000
nat-keepalive <10-3600>	Sets the global NAT keepalive interval from 10 - 3600 seconds
peer <IKEV1-PEER>	Specify the Name/Identifier for the IKEv1 peer. For IKEV1 peer configuration commands, see *crypto-ikev1/ikev2-peer commands*.
policy <IKEV1-POLICY-NAME>	Configures an ISKAMP policy. Specify the name of the policy. The local IKE policy and the peer IKE policy must have matching group settings for successful negotiations. For IKEV1 policy configuration commands, see *crypto-ikev1/ikev2-policy commands*.
remote-vpn	Specifies the IKEV1 remote-VPN server configuration (responder only)

```
crypto ikev2 [cookie-challenge-threshold <1-100>|dpd-keepalive <10-3600>|
dpd-retries <1-100>|nat-keepalive <10-3600>|peer <IKEV2-PEER>|
policy <IKEV2-POLICY-NAME>|remote-vpn]
```

ikev2	Configures the IKEv2 parameters
cookie-challenge-threshold <1-100>	Starts cookie challenge after half open IKE SAs exceeds the specified limit. Sets the limit from 1 - 100
dpd-keepalive <10-3600>	Sets the global DPD interval from 10 - 3600 seconds
dpd-retries <1-100>	Sets the global DPD retries count from 1 - 100
nat-keepalive <10-3600>	Sets the global NAT keepalive interval from 10 - 3600 seconds
peer <IKEV2-PEER>	Specify the Name/Identifier for the IKEv2 peer
policy <IKEV2-POLICY-NAME>	Configures an ISKAMP policy. Specify the policy name. The local IKE policy and the peer IKE policy must have matching group settings for successful negotiations.
remote-vpn	Specifies an IKEV2 remote-VPN server configuration (responder only)

```
crypto ipsec df-bit [clear|copy|set]
```

ipsec	Configures the *Internet Protocol Security* (IPSec) policy parameters
df-bit [clear|copy|set]	Configures DF bit handling for encapsulating header. The options are: • clear – Clears the DF bit in the outer header and ignores in the inner header • copy – Copies the DF bit from the inner header to the outer header • set – Sets the DF bit in the outer header

```
crypto ipsec security-association lifetime [kilobytes <500-2147483646>|
seconds <120-86400>]
```

ipsec	Configures the IPSec policy parameters

security-association	Configures the IPSec SAs parameters
lifetime [kilobyte |seconds]	Defines the IPSec SAs lifetime (in kilobytes and/or seconds). Values can be entered in both kilobytes and seconds, which ever limit is reached first, ends the SA. When the SA lifetime ends it is renegotiated as a security measure. • kilobytes – Specifies a volume-based key duration (minimum is 500 KB and maximum is 2147483646 KB) • <500-2147483646> – Specify a value from 500 - 2147483646 KB. • seconds – Specifies a time-based key duration (minimum is 120 seconds and maximum is 86400 seconds) • <120-86400> – Specify a value from 120 - 86400 seconds. The security association lifetime can be overridden under crypto maps.

`crypto ipsec transform-set <TRANSFORM-SET-TAG> [esp-3des|esp-aes|esp-aes-192|esp-aes-256|esp-des|esp-null] [esp-md5-hmac|esp-sha-hmac]`

ipsec	Configures the IPSec policy parameters
transform-set <TRANSFORM-SET-TAG>	Defines the transform set configuration (authentication and encryption) for securing data • <TRANSFORM-SET-TAG> – Specify the transform set name. Specify the transform set used by the IPSec transport connection to negotiate the transform algorithm.
esp-3des	Configures the ESP transform using 3DES cipher (168 bits). The transform set is assigned to a crypto map using the map's set transform-set command.
esp-aes	Configures the ESP transform using *Advanced Encryption Standard* (AES) cipher. The transform set is assigned to a crypto map using the map's set transform-set command.
esp-aes-192	Configures the ESP transform using AES cipher (192 bits). The transform set is assigned to a crypto map using the map's set transform-set command.
esp-aes-256	Configures the ESP transform using AES cipher (256 bits). The transform set is assigned to a crypto map using the map's set transform-set command.
esp-des	Configures the ESP transform using *Data Encryption Standard* (DES) cipher (56 bits). The transform set is assigned to a crypto map using the map's set transform-set command.
esp-null	Configures the ESP transform with no encryption
{esp-md5-hmac| esp-sha-hmac}	The following keywords are common to all transform sets: • esp-md5-hmac – Configures ESP transform using HMAC-MD5 authorization • esp-sha-hmac – Configures ESP transform using HMAC-SHA authorization

`crypto map <CRYPTO-MAP-TAG> <1-1000> [ipsec-isakmp {dynamic}|ipsec-manual]`

map <CRYPTO-MAP-TAG>	Configures the crypto map, a software configuration entity that selects data flows that require security processing. The crypto map also defines the policy for these data flows. • <CRYPTO-MAP-TAG> – Specify a name for the crypto map. The name should not exceed 32 characters. For crypto map configuration commands, see *crypto-map-config-commands*.
<1-1000>	Defines the crypto map entry sequence. Specify a value from 1 - 1000.
ipsec-isakmp {dynamic}	Configures IPSEC w/ISAKMP. • dynamic – Optional. Configures dynamic map entry (remote VPN configuration) for XAUTH with mode-config or ipsec-l2tp configuration
ipsec-manual	Configures IPSEC w/manual keying. Remote configuration is not allowed for manual crypto map

`crypto pki import crl <TRUSTPOINT-NAME> <URL> <1-168>`

pki	Configures certificate parameters. The *Public Key Infrastructure* (PKI) protocol creates encrypted public keys using digital certificates from certificate authorities.
import	Imports a trustpoint related configuration

crl <TRUSTPOINT-NAME>	Imports a *Certificate Revocation List* (CRL). Imports a trustpoint including either a private key and server certificate or a CA certificate or both • <TRUSTPOINT-NAME> – Specify the trustpoint name.
<URL>	Specify the CRL source address in the following format: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>:<passwd>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb<n>:/path/file
<1-168>	Sets command replay duration from 1 - 168 hours

`crypto plain-text-deny-acl-scope [global|interface]`

plain-text-deny-acl-scope	Configures plain-text-deny-acl-scope parameters
global	Applies the plain text deny ACL globally
interface	Applies the plain text deny ACL to the interface only

`crypto remote-vpn-client`

remote-vpn-client	Configures remote VPN client settings. For more information, see *crypto-remote-vpn-client commands*.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#crypto ipsec transform-set
tpsec-tag1 esp-aes-256 esp-md5-hmac
rfs7000-37FABE(config-profile-default-rfs7000)#crypto map map1 10 ipsec-isakmp
dynamic
rfs7000-37FABE(config-profile-default-rfs7000)#crypto
plain-text-deny-acl-scope interface

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
  bridge vlan 1
  tunnel-over-level2
  ip igmp snooping
  ip igmp snooping querier
 no autoinstall configuration
 no autoinstall firmware
 device-upgrade persist-images
 crypto ikev1 dpd-retries 1
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ipsec transform-set tpsec-tag1 esp-aes-256 esp-md5-hmac
 crypto map map1 10 ipsec-isakmp dynamic
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 crypto plain-text-deny-acl-scope interface
 interface radio1
 interface radio2
 interface up
rfs7000-37FABE(config-profile-default-rfs7000)#
```

```
rfs7000-37FABE(config-profile-default-rfs7000)#crypto ipsec transform-set
tag1 esp-null esp-md5-hmac

rfs7000-37FABE(config-profile-default-rfs7000-transform-set-tag1)#?
Crypto Ipsec Configuration commands:
  mode     Encapsulation mode (transport/tunnel)
  no       Negate a command or set its defaults

  clrscr   Clears the display screen
  commit   Commit all changes made in this session
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  revert   Revert changes
  service  Service Commands
  show     Show running system information
  write    Write running configuration to memory or terminal

rfs7000-37FABE(config-profile-default-rfs7000-transform-set-tag1)#
```

Related Commands:

no	Disables or reverts settings to their default

crypto-auto-ipsec-tunnel commands

crypto

Creates an auto IPSec VPN tunnel and changes the mode to auto-ipsec-secure mode for further configuration

Auto IPSec tunneling provides a secure tunnel between two networked peer controllers or service platforms and associated access points that are within a range of valid IP addresses. You can define which packets are sent within the tunnel, and how they are protected. When a tunnelled peer sees a sensitive packet, it creates a secure tunnel and sends the packet through the tunnel to its remote peer destination or associated access point.

Tunnels are sets of *Security Associations* (SA) between two peers. SAs define the protocols and algorithms applied to sensitive packets and specify the keying mechanisms used by tunnelled peers. SAs are unidirectional and exist in both the inbound and outbound direction. SAs are established per the rules and conditions of defined security protocols (AH or ESP).

Internet Key Exchange (IKE) protocol is a key management protocol standard used in conjunction with IPSec. IKE enhances IPSec by providing additional features, flexibility, and configuration simplicity for the IPSec standard. IKE enables secure communications without time consuming manual pre-configuration for auto IPSec tunneling.

```
rfs7000-37FABE(config-profile-default-rfs7000)#crypto auto-ipsec-secure
rfs7000-37FABE(config-profile-default-rfs7000-crypto-auto-ipsec-secure)#?
Crypto Auto IPSEC Tunnel commands:
  groupid       Local/Remote identity and Authentication credentials for Auto
                IPSec Secure IKE negotiation
  ike-lifetime  Set lifetime for ISAKMP security association
  ikev2         IKEv2 configuration commands
  ip            Internet Protocol config commands
  no            Negate a command or set its defaults
  remotegw      Auto IPSec Secure Remote Peer IKE
```

```
clrscr          Clears the display screen
commit          Commit all changes made in this session
do              Run commands from Exec mode
end             End current mode and change to EXEC mode
exit            End current mode and down to previous mode
help            Description of the interactive help system
revert          Revert changes
service         Service Commands
show            Show running system information
write           Write running configuration to memory or terminal

rfs7000-37FABE(config-profile-default-rfs7000-crypto-auto-ipsec-secure)#
```

The following table summarizes the crypto IPSec auto tunnel commands.

Command	Description	Reference
groupid	Specifies the identity string used for IKE authentication	page 589
ip	Enables the controller or service platform to uniquely identify APs and the hosts present in the AP's subnet	page 590
ike-lifetime	Configures the IKE SA's key lifetime in seconds	page 591
ikev2	Enables/disables the forced reauthentication of IKEv2 peer	page 592
remotegw	Defines the IKE version used for an auto IPSec tunnel using secure gateways	*page 7-592*
no	Negates a command or sets its default	page 593

groupid

crypto-auto-ipsec-tunnel commands

Specifies the identity string used for IKE authentication

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
groupid <WORD> [psk|rsa]
groupid <WORD> [psk [0 <WORD>|2 <WORD>|<WORD>]|rsa]
```

Parameters

```
groupid <WORD> [psk [0 <WORD>|2 <WORD>|<WORD>]|rsa]
```

<WORD>	Specify a string up to 64 characters. This is the group identity used for IKE exchange for auto IPSec secure peers. After providing a group ID, specify the authentication method used to authenticate peers on the auto IPSec secure tunnel. The options are: psk and rsa.
psk [0 <WORD>|2 <WORD>|<WORD>]	Configures the pre-shared key • 0 <WORD> – Enter a clear text key • 2 <WORD> – Enter an encrypted key • <WORD> – Specify a string value from 8 - 21 characters.
rsa	Configures the *Rivest-Shamir-Adleman* (RSA) key. RSA is an algorithm for public key cryptography. It is the first algorithm known to be suitable for signing, as well as encryption. This is the default setting.

NOTE
Only one group ID is supported on the controller or service platform. All APs, controllers, and service platform must use the same group ID.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-crypto-auto-ipsec-secure)#group
id
 motorolasolutions@123 rsa

rfs7000-37FABE(config-profile-default-rfs7000-crypto-auto-ipsec-secure)#show
context
 crypto auto-ipsec-secure
  groupid motorolasolutions@123 rsa
rfs7000-37FABE(config-profile-default-rfs7000-crypto-auto-ipsec-secure)#
```

ip

crypto-auto-ipsec-tunnel commands

Enables the controller to uniquely identify APs and the hosts present in the AP's subnet. This allows the controller to correctly identify the destination host and create a dynamic site-to-site VPN tunnel between the host and the private network behind the controller.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
ip nat crypto
```

Parameters

```
ip nat crypto
```

ip nat crypto	Enables unique identification of APs and the hosts present in each AP's subnet Providing a unique ID enables the access point, wireless controller, or service platform to uniquely identify the destination device. This is essential in networks where there are multiple APs behind a router, or when two (or more) APs behind two (or more) different routers have the same IP address. Further, the same subnet exists behind these APs. For example, let us consider a scenario where there are two APs (A and B) behind two routers (1 and 2). AP 'A' is behind router '1'. And AP 'B' is behind router '2'. Both these APs have the same IP address (192.168.13.8). The subnet behind APs A and B is also the same (100.1.1.0/24). In such a scenario the controller fails to uniquely identify the hosts present in either AP's subnet. For more information, see *remotegw* and *crypto*.

Example

```
rfs4000-229D58config-profile-testBrocade Mobility
RFS4000-crypto-auto-ipsec-secure)#ip nat crypto
rfs4000-229D58config-profile-testBrocade Mobility
RFS4000-crypto-auto-ipsec-secure)#

rfs4000-229D58config-profile-testBrocade Mobility
RFS4000-crypto-auto-ipsec-secure)#show context
 crypto auto-ipsec-secure
  remotegw ike-version ikev2 uniqueid
  ip nat crypto
rfs4000-229D58config-profile-testBrocade Mobility
RFS4000-crypto-auto-ipsec-secure)#
```

ike-lifetime

crypto-auto-ipsec-tunnel commands

Configures the IKE SA's key lifetime in seconds

The lifetime defines how long a connection (encryption/authentication keys) should last, from successful key negotiation to expiration. Two peers need not exactly agree on the lifetime, though if they do not, there is some clutter for a superseded connection on the peer defining the lifetime as longer.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
ike-lifetime <600-86400>
```

Parameters

```
ike-lifetime <600-86400>
```

ike-lifetime <600-86400>	Sets the IKE SA's key lifetime in seconds • <600-86400> – Specify a value fro m 600 - 86400 seconds.

Example

```
rfs4000-229D58(config-profile-testBrocade Mobility
RFS4000-crypto-auto-ipsec-secure)#ike-lifetime
 800

rfs4000-229D58(config-profile-testBrocade Mobility
RFS4000-crypto-auto-ipsec-secure)#show context

 crypto auto-ipsec-secure
  ike-lifetime 800
rfs4000-229D58(config-profile-testBrocade Mobility
RFS4000-crypto-auto-ipsec-secure)#
```

ikev2

crypto-auto-ipsec-tunnel commands

Enables/disables the forced IKEv2 peer re-authentication

In most IPSec tunnel configurations, the lifetime of IKE SAs between peers is limited. Once the IKE SA key expires it is renegotiated. In such a scenario, the IKEv2 tunnel peers may or may not reauthenticate themselves. When enabled, IKE tunnel peers have to reauthenticate each time the IKE SA is renegotiated.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
ikev2 peer reauth
```

Parameters

```
ikev2 peer reauth
```

ikev2 peer reauth	Enables IKEv2 peer re-authentication. When enabled, IKE tunnel peers are forced to reauthenticate each time the IKE key is renegotiated.

Example

```
rfs4000-229D58(config-profile-testBrocade Mobility
RFS4000-crypto-auto-ipsec-secure)#ikev2 peer reauth
```

remotegw

crypto-auto-ipsec-tunnel commands

Defines the IKE version used for auto IPSEC tunnel negotiation using a secure gateway

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
remotegw ike-version [ikev1-aggr|ikev1-main|ikev2] {uniqueid}
```

Parameters

```
remotegw ike-version [ikev1-aggr|ikev1-main|ikev2] {uniqueid}
```

remotegw ike-version	Configures the IKE version used for initiating auto IPSec tunnel with secure gateways
ikev1-aggr	Aggregation mode is used by the auto IPSec tunnel initiator to set up the connection
ikev1-main	Main mode is used by the auto IPSec tunnel initiator to establish the connection
ikev2	IKEv2 is the preferred method when wireless controller/AP only is used
uniqueid	This keyword is common to all of the above parameters. • uniqueid – Optional. Enables the assigning of a unique ID to APs (using this profile) behind a router by prefixing the MAC address to the groupid Providing a unique ID enables the access point, wireless controller, or service platform to uniquely identify the destination device. This is essential in networks where there are multiple APs behind a router, or when two (or more) APs behind two (or more) different routers have the same IP address. For example, let us consider a scenario where there are two APs (A and B) behind two routers (1 and 2). AP 'A' is behind router '1'. And AP 'B' is behind router '2'. Both these APs have the same IP address (192.168.13.8). In such a scenario, the controller fails to establish an Auto IPSec VPN tunnel to either APs, because it is unable to uniquely identify them. After enabling unique ID assignment, enable IKE unique ID check. For more information, see *crypto*.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-crypto-auto-ipsec-secure)#remot
egw ike
-version ikev2 uniqueid
rfs7000-37FABE(config-profile-default-rfs7000-crypto-auto-ipsec-secure)#

rfs7000-37FABE(config-profile-default-rfs7000-crypto-auto-ipsec-secure)#show
context

 crypto auto-ipsec-secure
  remotegw ike-version ikev2 uniqueid
rfs7000-37FABE(config-profile-default-rfs7000-crypto-auto-ipsec-secure)#
```

no

crypto-auto-ipsec-tunnel commands

Negates a command or set its defaults

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no [groupid|ike-lifetime|ikev2|ip]
```

Parameters

```
no [groupid|ike-lifetime|ikev2|ip]
```

groupid	Removes local/remote identity for auto IPSec IKE
ike-lifetime	Removes the ISAKMP associations' lifetime period
ikev2	Removes the need of peer re-authenticate in case of ike rekey
ip nat crypto	Disables unique identification of APs behind the NAT router

Example

```
The following example shows the Auto IPSec VLAN bridge settings before the
'no' command is executed:

rfs7000-37FABE(config-profile-default-rfs7000-crypto-auto-ipsec-secure)#show
context
 crypto auto-ipsec-secure
  groupid motorolasolutions@123 rsa
rfs7000-37FABE(config-profile-default-rfs7000-crypto-auto-ipsec-secure)#

rfs7000-37FABE(config-profile-default-rfs7000-crypto-auto-ipsec-secure)#no
groupid

The following example shows the Auto IPSec VLAN bridge settings after the 'no'
command is executed:

rfs7000-37FABE(config-profile-default-rfs7000-crypto-auto-ipsec-secure)#show
context
 crypto auto-ipsec-secure
rfs7000-37FABE(config-profile-default-rfs7000-crypto-auto-ipsec-secure)#


nx4500-5CFA2B(config-profile-testBrocade Mobility
RFS4000-crypto-auto-ipsec-secure)#no ikev2 peer
 reauth

nx4500-5CFA2B(config-profile-testBrocade Mobility
RFS4000-crypto-auto-ipsec-secure)#show context

 crypto auto-ipsec-secure
  no ikev2 peer reauth
  ike-lifetime 800
nx4500-5CFA2B(config-profile-testBrocade Mobility
RFS4000-crypto-auto-ipsec-secure)#

nx4500-5CFA2B(config-profile-testBrocade Mobility
RFS4000-crypto-auto-ipsec-secure)#no ike-lifetime

nx4500-5CFA2B(config-profile-testBrocade Mobility
RFS4000-crypto-auto-ipsec-secure)#show context

 crypto auto-ipsec-secure
  no ikev2 peer reauth
nx4500-5CFA2B(config-profile-testBrocade Mobility
RFS4000-crypto-auto-ipsec-secure)#
```

crypto-ikev1/ikev2-policy commands

crypto

Defines crypto-IKEv1/IKEv2 commands in detail

IKE protocol is a key management protocol standard used in conjunction with IPSec. IKE enhances IPSec by providing additional features, flexibility, and configuration simplicity for the IPSec standard. IKE automatically negotiates IPSec SAs, and enables secure communications without time consuming manual pre-configuration.

Use the (config) instance to configure IKEv1/IKEv2 policy configuration commands. To navigate to the IKEv1 policy config instance, use the following commands:

```
<DEVICE>(config)#profile <DEVICE-TYPE> <PROFILE-NAME>
<DEVICE>(config-profile-<PROFILE-NAME>)#crypto ikev1/ikev2 policy
<IKEV1/IKEV2-POLICY-NAME>

rfs7000-37FABE(config-profile-default-rfs7000)#crypto ikev1 policy
ikev1-testpolicy
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-ikev1-testpolicy)#
?
Crypto IKEv1 Policy Configuration commands:
  dpd-keepalive    Set Dead Peer Detection interval in seconds
  dpd-retries      Set Dead Peer Detection retries count
  isakmp-proposal  Configure ISAKMP Proposals
  lifetime         Set lifetime for ISAKMP security association
  mode             IKEv1 mode (main/aggressive)
  no               Negate a command or set its defaults

  clrscr           Clears the display screen
  commit           Commit all changes made in this session
  end              End current mode and change to EXEC mode
  exit             End current mode and down to previous mode
  help             Description of the interactive help system
  revert           Revert changes
  service          Service Commands
  show             Show running system information
  write            Write running configuration to memory or terminal

rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-ikev1-testpolicy)#

rfs7000-37FABE(config-profile-test-ikev2-policy-ikev2-testpolicy)#?
Crypto IKEv2 Policy Configuration commands:
  dpd-keepalive    Set Dead Peer Detection interval in seconds
  isakmp-proposal  Configure ISAKMP Proposals
  lifetime         Set lifetime for ISAKMP security association
  no               Negate a command or set its defaults
  sa-per-acl       Setup single SA for all rules in the ACL (ONLY APPLICABLE
                   FOR SITE-TO-SITE VPN)

  clrscr           Clears the display screen
  commit           Commit all changes made in this session
  do               Run commands from Exec mode
  end              End current mode and change to EXEC mode
  exit             End current mode and down to previous mode
  help             Description of the interactive help system
  revert           Revert changes
  service          Service Commands
  show             Show running system information
```

```
  write            Write running configuration to memory or terminal

rfs7000-37FABE(config-profile-test-ikev2-policy-ikev2-testpolicy)#
```

NOTE
IKEv2 being an improved version of the original IKEv1 design, is recommended in most deployments. IKEv2 provides enhanced cryptographic mechanisms, NAT and firewall traversal, attack resistance etc.

The following table summarizes crypto IKEv1/iKEv2 commands.

Command	Description	Reference
dpd-keepalive	Sets DPD keep alive packet interval	page 596
dpd-retries	Sets the maximum number of attempts for sending *Dead-Peer-Detection* (DPD) keep alive packets (applicable only to the IKEv1 policy)	*page 7-597*
isakmp-proposal	Configures ISAKMP proposals	*page 7-597*
lifetime	Specifies how long an IKE SA is valid before it expires	*page 7-598*
mode	Sets the mode of the tunnels (applicable only to the IKEv1 policy)	*page 7-599*
no	Negates a command or sets its default	*page 7-600*

dpd-keepalive

crypto-ikev1/ikev2-policy commands

Sets the DPD keep-alive packet interval

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
dpd-keepalive <10-3600>
```

Parameters

```
dpd-keepalive <10-3600>
```

<10-3600>	Specifies the interval, in seconds, between successive DPD keep alive packets.The IKE keep alive message interval is used to detect a dead peer on the remote end of the IPSec VPN tunnel. Specify the time from 10 - 3600 seconds. The default is 30 seconds

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-ikev1-testpolicy)#
dpd-keepalive 11

rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-testpolicy)#show
context
 crypto ikev1 policy testpolicy
```

```
  dpd-keepalive 11
  isakmp-proposal default encryption aes-256 group 2 hash sha
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-testpolicy)#
```

dpd-retries

crypto-ikev1/ikev2-policy commands

Sets the maximum number of attempts for sending DPD keep alive packets to a peer. Once this value is exceeded, without a response, the VPN tunnel connection is declared dead. This option is available only for the IKEv1 policy.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
dpd-retries <1-100>
```

Parameters

```
dpd-retries <1-100>
```

<1-100>	Declares a peer dead after the specified number of retries. Specify a value from 1-100.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-testpolicy)#dpd-re
tries 10

rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-testpolicy)#show
context
 crypto ikev1 policy testpolicy
  dpd-keepalive 11
  dpd-retries 10
  isakmp-proposal default encryption aes-256 group 2 hash sha
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-testpolicy)#
```

isakmp-proposal

crypto-ikev1/ikev2-policy commands

Configures ISAKMP proposals and their parameters

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
isakmp-proposal <WORD> encryption [3des|aes|aes-192|aes-256] group [14|2|5]
          hash [md5|sha]
```

Parameters

```
isakmp-proposal <WORD> encryption [3des|aes|aes-192|aes-256] group [14|2|5]
hash [md5|sha]
```

<WORD>	Specify the name of the ISAKMP proposal
encryption [3des|aes| aes-192|aes-256]	Configures the encryption level transmitted using the crypto isakmp command • 3des – Configures triple data encryption standard • aes – Configures AES (128 bit keys) • aes-192 – Configures AES (192 bit keys) • aes-256 – Configures AES (256 bit keys)
group [14|2|5]	Specifies the *Diffie-Hellman* (DH) group (1 or 2) used by the IKE policy to generate keys (used to create IPSec SA). Specifying the group enables you to declare the modulus size used in DH calculation. • 14 – Configures DH group 14 • 2 – Configures DH group 2 • 5 – Configures DH group 5
hash [md5|sha]	Specifies the hash algorithm used to authenticate data transmitted over the IKE SA • md5 – Uses *Message Digest 5* (MD5) hash algorithm • sha – Uses *Secure Hash Authentication* (SHA) hash algorithm

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-ikev1-testpolicy)#
isakmp-proposal testproposal encryption aes group 2 hash sha

rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-testpolicy)#show
context
 crypto ikev1 policy testpolicy
  dpd-keepalive 11
  dpd-retries 10
  isakmp-proposal default encryption aes-256 group 2 hash sha
  isakmp-proposal testpraposal encryption aes group 2 hash sha
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-testpolicy)#
```

lifetime

crypto-ikev1/ikev2-policy commands

Specifies how long an IKE SA is valid before it expires

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
lifetime <600-86400>
```

Parameters

```
lifetime <600-86400>
```

<lifetime 600-86400>	Specifies how many seconds an IKE SA lasts before it expires. Set a time stamp from 600 - 86400 seconds. • <600-86400> – Specify a value from 600 -8 6400 seconds.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-test-ikev1policy)#
lifetime 655

rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-testpolicy)#show
context
 crypto ikev1 policy testpolicy
  dpd-keepalive 11
  dpd-retries 10
  lifetime 655
  isakmp-proposal default encryption aes-256 group 2 hash sha
  isakmp-proposal testpraposal encryption aes group 2 hash sha
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-testpolicy)#
```

mode

crypto-ikev1/ikev2-policy commands

Configures the IPSec mode of operation for the IKEv1 policy

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
mode [aggresive|main]
```

Parameters

```
mode [aggresive|main]
```

mode [aggresive|main]	Sets the mode of the tunnels • aggressive – Initiates the aggressive mode • main – Initiates the main mode If configuring the IKEv1 IPSec policy, define the IKE mode as either *main* or *aggressive.* In the aggressive mode, 3 messages are exchanged between the IPSec peers to setup the SA. On the other hand, in the main mode, 6 messages are exchanged. The default setting is main.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-testpolicy)#mode
aggressive

rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-testpolicy)#show
context
 crypto ikev1 policy testpolicy
```

```
  dpd-keepalive 11
  dpd-retries 10
  lifetime 655
  isakmp-proposal default encryption aes-256 group 2 hash sha
  isakmp-proposal testpraposal encryption aes group 2 hash sha
  mode aggressive
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-testpolicy)#
```

no

crypto-ikev1/ikev2-policy commands

Negates a command or set its defaults

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no [dpd-keepalive|dpd-retries|isakmp-proposal|lifetime|mode]
```

Parameters

```
no [dpd-keepalive|dpd-retries|isakmp-proposal|lifetime|mode]
```

dpd-keepalive	Resets the DPD keepalive interval to default
dpd-retries	Resets the DPD keepalive retries count to default (applicable only to the IKEv1 policy)
isakmp-proposal	Removes the configured ISAKMP proposal
lifetime	Resets the ISAKMP security association lifetime
mode	Resets the tunnelling mode to default (main mode) (applicable only to the IKEv1 policy)

Example

```
The following example shows the IKEV1 Policy settings before the ‘no’ commands
are executed:

rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-testpolicy)#show
context
 crypto ikev1 policy testpolicy
  dpd-keepalive 11
  dpd-retries 10
  lifetime 655
  isakmp-proposal default encryption aes-256 group 2 hash sha
  isakmp-proposal testpraposal encryption aes group 2 hash sha
  mode aggressive
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-testpolicy)#

rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-testpolicy)#no
mode
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-testpolicy)#no
dpd-keepalive
```

```
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-testpolicy)#no
dpd-retries

The following example shows the IKEV1 Policy settings after the ‘no’ commands
are executed:

rfs7000-37FABEconfig-profile-default-rfs7000-ikev1-policy-testpolicy)#show
context
 crypto ikev1 policy testpolicy
  lifetime 655
  isakmp-proposal default encryption aes-256 group 2 hash sha
  isakmp-proposal testpraposal encryption aes group 2 hash sha
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-testpolicy)#
```

crypto-ikev1/ikev2-peer commands

crypto

Use the (config) instance to configure IKEv1/IKEv2 peer configuration commands. To navigate to the IKEv1 peer config instance, use the following commands:

```
<DEVICE>(config)#profile <DEVICE-TYPE> <PROFILE-NAME>
<DEVICE>(config-profile-<PROFILE-NAME>)#crypto ikev1/ikev2 peer
<IKEV1/IKEV2-PEER-NAME>

rfs7000-37FABE(config-profile-default-rfs7000)#crypto ikev1 peer peer1
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#?
Crypto IKEV1 Peer Configuration commands:
  authentication  Configure Authentication credentials
  ip              Configure peer address/fqdn
  localid         Set local identity
  no              Negate a command or set its defaults
  remoteid        Configure remote peer identity
  use             Set setting to use

  clrscr          Clears the display screen
  commit          Commit all changes made in this session
  end             End current mode and change to EXEC mode
  exit            End current mode and down to previous mode
  help            Description of the interactive help system
  revert          Revert changes
  service         Service Commands
  show            Show running system information
  write           Write running configuration to memory or terminal

rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#

rfs7000-37FABE(config-profile-default-rfs7000)#crypto ikev2 peer peer1
rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#?
Crypto IKEV2 Peer Configuration commands:
  authentication  Configure Authentication credentials
  ip              Configure peer address/fqdn
  localid         Set local identity
  no              Negate a command or set its defaults
  remoteid        Configure remote peer identity
  use             Set setting to use

  clrscr          Clears the display screen
  commit          Commit all changes made in this session
  do              Run commands from Exec mode
```

```
  end             End current mode and change to EXEC mode
  exit            End current mode and down to previous mode
  help            Description of the interactive help system
  revert          Revert changes
  service         Service Commands
  show            Show running system information
  write           Write running configuration to memory or terminal

rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#
```

The following table summarizes crypto IPSec IKEv1/IKEv2 peer configuration commands.

Command	Description	Reference
authentication	Configures a peer's authentication mode and credentials	page 602
ip	Configures the peer's IP address	*page 7-603*
localid	Configures a peer's local identity details	page 604
remoteid	Configures a remote peer's identity details	page 604
use	Associates a IKEv1 policy and IKEv2 policy with the IKEv1 and IKEv2 peer respectively	page 605
no	Negates a command or reverts settings to their default. The no command, when used in the ISAKMP policy mode, defaults the ISAKMP protection suite settings.	page 606

authentication

crypto-ikev1/ikev2-peer commands

Configures IKEv1/IKEv2 peer's authentication mode and credentials

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
authentication [psk|rsa]

authentication psk [0 <WORD>|2 <WORD>|<WORD>]
```

Parameters

```
authentication [psk [0 <WORD>|2 <WORD>|<WORD>]|rsa]
```

psk [0 <WORD>| 2 <WORD>|<WORD>	Configures *pre-shared key* (PSK) authentication method • 0 <WORD> – Specifies a clear text key. The key must be from 8 - 21 characters • 2 <WORD> – Specifies an encrypted key. The key must be from 8 - 21 characters • <WORD> – Pre-shared key. The key must be from 8 - 21 characters
rsa	Configures RSA-SIG authentication method

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#authenticatio
n rsa
```

```
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#

rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#authenticatio
n
psk 0 moto@123456

rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#show context
 crypto ikev2 peer peer1
  authentication psk 0 moto@123456 local
  authentication psk 0 moto@123456 remote
rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#
```

ip

crypto-ikev1/ikev2-peer commands

Sets the IP address of the peer device. This can be set for multiple remote peers. The remote peer can be either an IP address or hostname.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
ip [address <IP>|fqdn <WORD>]
```

Parameters

```
ip [address <IP>|fqdn <WORD>]
```

address <IP>	Specify the peer device's IP address.
fqdn <WORD>	Specify the peer device's FQDN hostname.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#ip address
172.16.10.12

rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#show context
 crypto ikev1 peer peer1
  ip address 172.16.10.12
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#

rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#ip address
192.168.10.6

rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#show context
 crypto ikev2 peer peer1
  ip address 192.168.10.6
  authentication psk 0 moto@123456 local
  authentication psk 0 moto@123456 remote
rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#
```

localid

crypto-ikev1/ikev2-peer commands

Sets a IKEv1/IKEv2 peer's local identity credentials

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
localid [address|dn|email|fqdn|string]
localid [address <IP>|dn <WORD>|email <WORD>|fqdn <WORD>|string <WORD>]

The following command is specific to the IKEv2 peer configuration:

localid autogen-uniqueid <WORD>
```

Parameters

```
localid [address <IP>|dn <WORD>|email <WORD>|fqdn <WORD>|string <WORD>]
```

address <IP>	Configures the peer's IP address. The IP address is used as local identity.
dn <WORD>	Configures the peer's distinguished name. (for example, "C=us ST=<state> L=<location> O=<organization> OU=<org unit>". The maximum length is 128 characters.
email <WORD>	Configures the peer's e-mail address. The maximum length is 128 characters.
fqdn <WORD>	Configures the peer's FQDN. The maximum length is 128 characters.
string <WORD>	Configures the peer's identity string. The maximum length is 128 characters.

```
localid autogen-uniqueid <WORD>
```

autogen-uniqueid <WORD>	Prefixes the autogen-uniqueid of the device to the string provided here. The device's autogen-uniqueid should be existing and configured. For more information on autogen-uniqueid, see *autogen-uniqueid*. • <WORD> – Provide the string that is prefixed to the device's autogen-uniqueid.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#localid email
bob@motorolasolutions.com

rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#show context
 crypto ikev1 peer peer1
  ip address 172.16.10.12
  localid email bob@motorolasolutions.com
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#
```

remoteid

crypto-ikev1/ikev2-peer commands

Configures a IKEv1/IKEV2 peer's remote identity credentials

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
remoteid [address <IP>|dn <WORD>|email <WORD>|fqdn <WORD>|string <WORD>]
```

Parameters

```
remoteid [address <IP>|dn <WORD>|email <WORD>|fqdn <WORD>|string <WORD>]
```

address <IP>	Configures the remote IKEv1/IKEV2 peer's IP address. The IP address is used as the peer's remote identity.
dn <WORD>	Configures the remote peer's distinguished name. For example, "C=us ST=<state> L=<location> O=<organization> OU=<org unit>". The maximum length is 128 characters.
email <WORD>	Configures the remote peer's e-mail address. The maximum length is 128 characters.
fqdn <WORD>	Configures a peer's FQDN. The maximum length is 128 characters.
string <WORD>	Configures a peer's identity string. The maximum length is 128 characters.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#remoteid dn
San
Jose

rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#show context
 crypto ikev1 peer peer1
  ip address 172.16.10.12
  remoteid dn SanJose
  localid email bob@motorolasolutions.com
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#

rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#remoteid
address 157.235.209.63

rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#show context
 crypto ikev2 peer peer1
  remoteid address 157.235.209.63
rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#
```

use

crypto-ikev1/ikev2-peer commands

Associates IKEv1/IKEv2 policy configuration settings with IKEv1/IKEv2 peer

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
use ikev1-policy <IKEV1-POLICY-NAME>
use ikev2-policy <IKEV2-POLICY-NAME>
```

Parameters

```
use ikev1-policy <IKEV1-POLICY-NAME>
```

use ikev1-policy <IKEV1-POLICY-NAME>	Specify the IKEv1 policy name. The local IKE policy and the peer IKE policy must have matching group settings for successful negotiations.

```
use ikev2-policy <IKEV2-POLICY-NAME>
```

use ikev2-policy <IKEV2-POLICY-NAME>	Specify the IKEv2 policy name. The local IKE policy and the peer IKE policy must have matching group settings for successful negotiations.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#use
ikev1-policy test-ikev1policy

rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#show context
 crypto ikev1 peer peer1
  ip address 172.16.10.12
  remoteid dn SanJose
  localid email bob@motorolasolutions.com
  use ikev1-policy test-ikev1policy
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#

rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#use
ikev2-policy test-ikev2policy

rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#show context
 crypto ikev2 peer peer1
  remoteid address 157.235.209.63
  use ikev2-policy test-ikev2policy
rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#
```

no

crypto-ikev1/ikev2-peer commands

Removes or reverts IKEv1/IKEv2 peer settings

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no [authentication|ip|localid|remoteid|use]
```

Parameters

```
no [authentication|ip|localid|remoteid|use]
```

no authentication	Removes a IKEv1/IKEv2 peer's authentication credentials
no ip	Removes a IKEv1/IKEv2 peer's IP address / FQDN
no localid	Removes a IKEv1/IKEv2 peer's local identity details
no remoteid	Removes a IKEv1/IKEv2 peer's remote identity details
no use	Removes the IKEv1/IKEv2 policy associated with IKEv1/IKEv2 peer respectively

Example

```
The following example shows the Crypto IKEV1 peer1 settings before the 'no'
commands are executed:

rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#show context
 crypto ikev1 peer peer1
  ip address 172.16.10.12
  remoteid dn SanJose
  localid email bob@motorolasolutions.com
  use ikev1-policy test-ikev1policy
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#

rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#no localid
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#no remoteid

The following example shows the Crypto IKEV1 peer1 settings after the 'no'
commands are executed:

rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#show context
 crypto ikev1 peer peer1
  ip address 172.16.10.12
  use ikev1-policy test-ikev1policy
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#

The following example shows the Crypto IKEV2 peer1 settings before the 'no'
commands are executed:

rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#show context
 crypto ikev2 peer peer1
  remoteid address 157.235.209.63
  use ikev2-policy test
rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#

The following example shows the Crypto IKEV2 peer1 settings after the 'no'
commands are executed:

rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#no use
ikev2-policy

rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#show context
 crypto ikev2 peer peer1
  remoteid address 157.235.209.63
rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#
```

crypto-map-config-commands

crypto

This section explains crypto map commands in detail.

A crypto map entry is a single policy that describes how certain traffic is secured. There are two types of crypto map entries: ipsec-manual and ipsec-ike. Each entry is given an index (used to sort the ordered list).

IPSec VPN provides a secure tunnel between two networked peers. Administrators can define which packets are sent within the tunnel, and how they're protected. When a tunneled peer sees a sensitive packet, it creates a secure tunnel and sends the packet through the tunnel to its remote peer destination.

Tunnels are sets of SA between two peers. SAs define the protocols and algorithms applied to sensitive packets and specify the keying mechanisms used by tunneled peers. SAs are unidirectional and exist in both the inbound and outbound direction. SAs are established per the rules and conditions of defined security protocols (AH or ESP).

Internet Key Exchange (IKE) protocol is a key management protocol standard used in conjunction with IPSec. IKE enhances IPSec by providing additional features, flexibility, and configuration simplicity for the IPSec standard. IKE automatically negotiates IPSec SAs, and enables secure communications without time consuming manual pre-configuration.

Use crypto maps to configure IPSec VPN SAs. Crypto maps combine the elements comprising IPSec SAs. Crypto maps also include transform sets. A transform set is a combination of security protocols, algorithms and other settings applied to IPSec protected traffic. One crypto map is utilized for each IPsec peer, however for remote VPN deployments one crypto map is used for all the remote IPsec peers.

Use the (config) instance to enter the crypto map configuration mode. To navigate to the crypto-map configuration instance, use the following commands:

```
In the device-config mode:
<DEVICE>(config-device-<DEVICE-MAC>)#crypto map <CRYPTO-MAP-TAG> <1-1000>
          [ipsec-isakmp {dynamic}|ipsec-manual]

In the profile-config mode:
<DEVICE>(config-profile-<PROFILE-NAME>)#crypto map <CRYPTO-MAP-TAG> <1-1000>
          [ipsec-isakmp {dynamic}|ipsec-manual]
```

There are three different configurations defined for each listed crypto map: site-to-site manual (ipsec-manual), site-to-site-auto tunnel (ipsec-isakmp), and remote VPN client (ipsec-isakmp dynamic). With site-to-site deployments, an IPSEC tunnel is deployed between two gateways, each at the edge of two different remote networks. With remote VPN, an access point located at remote branch defines a tunnel with a security gateway. This facilitates the end points in the branch office to communicate with the destination endpoints (behind the security gateway) in a secure manner.

Each crypto map entry is given an index (used to sort the ordered list).

```
rfs7000-37FABE(config-profile-default-rfs7000)#crypto map map1 1 ipsec-manual
rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#?
Manual Crypto Map Configuration commands:
  local-endpoint-ip     Use this IP as local tunnel endpoint address, instead
                        of the interface IP (Advanced Configuration)
  mode                  Set the tunnel mode
  no                    Negate a command or set its defaults
  peer                  Set peer
  security-association  Set security association parameters
  session-key           Set security session key parameters
  use                   Set setting to use

  clrscr                Clears the display screen
```

```
  commit                Commit all changes made in this session
  do                    Run commands from Exec mode
  end                   End current mode and change to EXEC mode
  exit                  End current mode and down to previous mode
  help                  Description of the interactive help system
  revert                Revert changes
  service               Service Commands
  show                  Show running system information
  write                 Write running configuration to memory or terminal

rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#
```

The following table summarizes crypto map configuration mode commands.

Command	Description	Reference
crypto-map auto-vpn-tunnel/remote-vpn-client instance	Configures an auto site-to-site VPN or remote VPN client	page 609
crypto-map-ipsec-manual-instance	Configures a manual site-to-site VPN	page 621

crypto-map auto-vpn-tunnel/remote-vpn-client instance

crypto-map-config-commands

To navigate to the auto site-to-site VPN tunnel configuration instance, use the following command:

```
In the device-config mode:
<DEVICE>(config-device-<DEVICE-MAC>)#crypto map <CRYPTO-MAP-TAG> <1-1000>
ipsec-isakmp

In the profile-config mode:
<DEVICE>(config-profile-<PROFILE-NAME>)#crypto map <CRYPTO-MAP-TAG> <1-1000>
          ipsec-isakmp

rfs4000-229D58(config-device-00-23-68-22-9D-58)#crypto map test 1 ipsec-isakmp
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#?
Site to Site Crypto Map Configuration commands:
  ip                    Internet Protocol config commands
  local-endpoint-ip     Use this IP as local tunnel endpoint address, instead
                        of the interface IP (Advanced Configuration)
  no                    Negate a command or set its defaults
  peer                  Add a remote peer
  pfs                   Specify Perfect Forward Secrecy
  security-association  Security association parameters
  transform-set         Specify IPSec transform to use
  use                   Set setting to use

  clrscr                Clears the display screen
  commit                Commit all changes made in this session
  do                    Run commands from Exec mode
  end                   End current mode and change to EXEC mode
  exit                  End current mode and down to previous mode
  help                  Description of the interactive help system
  revert                Revert changes
  service               Service Commands
  show                  Show running system information
```

```
  write                Write running configuration to memory or terminal

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#
```

To navigate to the remote VPN client configuration instance, use the following command:

```
In the device-config mode:
<DEVICE>(config-device-<DEVICE-MAC>)#crypto map <CRYPTO-MAP-TAG> <1-1000>
ipsec-isakmp
          {dynamic}

In the profile-config mode:
<DEVICE>(config-profile-<PROFILE-NAME>)#crypto map <CRYPTO-MAP-TAG> <1-1000>
          ipsec-isakmp {dynamic}

rfs4000-229D58(config-device-00-23-68-22-9D-58)#crypto map test 2 ipsec-isakmp
dynamic
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#?
Dynamic Crypto Map Configuration commands:
  local-endpoint-ip     Use this IP as local tunnel endpoint address, instead
                        of the interface IP (Advanced Configuration)
  modeconfig            Set the mode config method
  no                    Negate a command or set its defaults
  peer                  Add a remote peer
  pfs                   Specify Perfect Forward Secrecy
  remote-type           Set the remote VPN client type
  security-association  Security association parameters
  transform-set         Specify IPSec transform to use
  use                   Set setting to use

  clrscr                Clears the display screen
  commit                Commit all changes made in this session
  do                    Run commands from Exec mode
  end                   End current mode and change to EXEC mode
  exit                  End current mode and down to previous mode
  help                  Description of the interactive help system
  revert                Revert changes
  service               Service Commands
  show                  Show running system information
  write                 Write running configuration to memory or terminal

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
```

The following table lists the IPSec-Auto-VPN/Remote-VPN tunnel configuration commands:

Command	Description	Reference
ip	Enables this setting to utilize IP/Port NAT on the VPN tunnel. This command is applicable only to the site-to-site VPN tunnel.	page 611
local-endpoint-ip	Uses the configured IP as local tunnel endpoint address, instead of the interface IP. This command is applicable to the site-to-site VPN tunnel and remote VPN client.	page 611
modeconfig	Configures the mode config method (pull or push) associated with the remote VPN client. This command is applicable only to the remote VPN client.	page 612
peer	Configures the IKEv1 or IKEv2 peer for the VPN tunnel. This command is applicable to the site-to-site VPN tunnel and remote VPN client.	page 613
pfs	Configures the *Perfect Forward Secrecy* (PFS) for the VPN tunnel. This command is applicable to the site-to-site VPN tunnel and remote VPN client.	page 614

Command	Description	Reference
remote-type	Configures the remote VPN client type as either None or XAuth. This command is applicable only to the remote VPN client.	page 615
security-association	Defines this automatic VPN tunnel's IPSec SA settings. This command is applicable to the site-to-site VPN tunnel and remote VPN client.	page 616
transform-set	Applies a transform set (encryption and hash algorithms) to the VPN tunnel. This command is applicable to the site-to-site VPN tunnel and remote VPN client.	page 617
use	Applies an existing and configured IP access list to the VPN tunnel. This command is applicable to the site-to-site VPN tunnel and remote VPN client.	page 618
no	Removes or reverts site-to-site VPN tunnel or remote VPN client settings	page 619

ip

crypto-map auto-vpn-tunnel/remote-vpn-client instance

Enables this setting to utilize IP/Port NAT on this auto site-to-site VPN tunnel. This setting is disabled by default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
ip nat crypto
```

Parameters

```
ip nat crypto
```

ip nat crypto	Enables this setting to utilize IP/Port NAT on the site-to-site VPN tunnel. This setting is disabled by default.

Example

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#ip nat
crypto

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#show context
 crypto map test 1 ipsec-isakmp
  ip nat crypto
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#
```

local-endpoint-ip

crypto-map auto-vpn-tunnel/remote-vpn-client instance

Uses the configured IP as local tunnel endpoint address, instead of the interface IP

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
local-endpoint-ip <IP>
```

Parameters

```
local-endpoint-ip <IP>
```

local-endpoint-ip <IP>	Configures the local VPN tunnel's (site-to-site VPN tunnel or remote VPN client) endpoint IP address • <IP> – Specify the IP address. The specified IP address must be available on the interface.

Example

```
Site-to-site VPN tunnel:

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#local-endpoi
nt-ip 192.168.13.10

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#show context
 crypto map test 1 ipsec-isakmp
  local-endpoint-ip 192.168.13.10
  ip nat crypto
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#

Remote VPN client:

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#local-endpoi
nt-ip 157.235.204.62

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context
 crypto map test 2 ipsec-isakmp dynamic
  local-endpoint-ip 157.235.204.62
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
```

modeconfig

crypto-map auto-vpn-tunnel/remote-vpn-client instance

Configures the mode config method (pull or push) associated with the remote VPN client

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
modeconfig [pull|push]
```

Parameters

```
modeconfig [pull|push]
```

modeconfig [pull|push]	Configures the mode config method associated with a remote VPN client. The options are: pull and push. The mode (pull or push) defines the method used to assign a virtual IP. This setting is relevant for IKEv1 only, since IKEv2 always uses the configuration payload in pull mode. The default setting is push.

Example

```
Remote VPN client:

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#modeconfig
push
```

peer

crypto-map auto-vpn-tunnel/remote-vpn-client instance

Configures the IKEv1 or IKEv2 peer for the auto site-to-site VPN tunnel or remote VPN client. The peer device can be specified either by its hostname or by its IP address. A maximum of three peers can be configured.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
peer <1-3> [ikev1|ikev2] <IKEv1/IKEv2-PEER-NAME>
```

Parameters

```
peer <1-3> [ikev1|ikev2] <IKEv1/IKEv2-PEER-NAME>]
```

peer <1-3>	Creates a new peer and configures the peer's priority level. Peer '1' is the primary peer, and peer '3' is redundant.
ikev1 <IKEv1-PEER-NAME>	Configures an IKEv1 peer • <IKEv1-PEER-NAME> – Specify the IKEv1 peer's name.
ikev2<IKEv2-PEER-NAME>	Configures an IKEv2 peer • <IKEv2-PEER-NAME> – Specify the IKEv2 peer's name.

Example

```
Site-to-site tunnel:

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#peer 1 ikev2
ikev2Peer1

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#show context
 crypto map test 1 ipsec-isakmp
  peer 1 ikev2 ikev2Peer1
  local-endpoint-ip 192.168.13.10
  ip nat crypto
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#
```

```
Remote VPN client:

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#peer 1 ikev1
Re
moteIKEv1Peer1

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context
 crypto map test 2 ipsec-isakmp dynamic
  peer 1 ikev1 RemoteIKEv1Peer1
  local-endpoint-ip 157.235.204.62
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
```

pfs

crypto-map auto-vpn-tunnel/remote-vpn-client instance

Configures the *Perfect Forward Secrecy* (PFS) for the auto site-to-site VPN tunnel or remote VPN client

PFS is key-establishment protocol, used to secure VPN communications. If one encryption key is compromised, only data encrypted by that specific key is compromised. For PFS to exist, the key used to protect data transmissions must not be used to derive any additional keys. Options include 2, 5 and 14. The option is disabled by default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
pfs [14|2|5]
```

Parameters

```
pfs [14|2|5]
```

pfs [14|2|5]	Configures the PFS • 14 – Configures D-H Group14 (2048-bit modp) • 2 – Configures D-H Group2 (1024-bit modp) • 5 – D-H Group5 (1536-bit modp)

Example

```
Site-to-site VPN tunnel:

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#pfs 5

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#show context
 crypto map test 1 ipsec-isakmp
  peer 1 ikev2 ikev2Peer1
  local-endpoint-ip 192.168.13.10
  pfs 5
  ip nat crypto
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#
```

```
Remote VPN client:

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#pfs 14

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context
 crypto map test 2 ipsec-isakmp dynamic
  peer 1 ikev1 RemoteIKEv1Peer1
  local-endpoint-ip 157.235.204.62
  pfs 14
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
```

remote-type

crypto-map auto-vpn-tunnel/remote-vpn-client instance

Configures the remote VPN client type as either None or XAuth

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
remote-type [none|xauth]
```

Parameters

```
remote-type [none|xauth]
```

remote-type [none|xauth]	Specify the remote VPN's client type • none – Specifies remote VPN client with No XAUTH • xauth – Specify remote VPN client as using XAUTH (applicable only for IKEv1). This is the default setting XAuth (extended authentication) provides additional authentication validation by permitting an edge device to request extended authentication information from an IPSec host. This forces the host to respond with additional authentication credentials. The edge device respond with a failed or passed message. The default setting is XAuth.

Example

```
Remote VPN client:

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#remote-type
none

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context
 crypto map test 2 ipsec-isakmp dynamic
  peer 1 ikev1 RemoteIKEv1Peer1
  local-endpoint-ip 157.235.204.62
  pfs 14
  remote-type none
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
```

security-association

crypto-map auto-vpn-tunnel/remote-vpn-client instance

Defines the IPSec SA's (created by this auto site-to-site VPN tunnel or remote VPN client) settings

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
security-association [inactivity-timeout|level|lifetime]

security-association [inactivity-timeout <120-86400>|level prehost]
security-association lifetime [kilobytes <500-2147483646>|seconds <120-86400>]
```

Parameters

```
security-association [inactivity-timeout <120-86400>|level prehost]
```

inactivity-timeout <120-86400>	Specifies an inactivity period, in seconds, for this IPSec VPN SA. Once the set value is exceeded, the association is timed out. • <120-86400> – Specify a value from 120 - 86400 seconds. The default is 900 seconds.
level prehost	Specifies the granularity level for this IPSec VPN SA • prehost – Sets the IPSec VPN SA's granularity to the host level

```
security-association lifetime [kilobytes <500-2147483646>|seconds <120-86400>]
```

lifetime [kilobytes <500-2147483646>| seconds <120-86400>]	Defines the IPSec SA's lifetime (in kilobytes and/or seconds). Values can be entered in both kilobytes and seconds. Which ever limit is reached first, ends the security association. • kilobytes <500-2147483646> – Defines volume based key duration. Specify a value from 500 - 2147483646 kilobytes. Select this option to define a connection volume lifetime (in kilobytes) for the duration of the IPSec VPN SA. Once the set volume is exceeded, the association is timed out. • seconds <120-86400> – Defines time based key duration. Specify the time frame from 120 - 86400 seconds. Select this option to define a lifetime (in seconds) for the duration of the IPSec VPN SA. Once the set value is exceeded, the association is timed out.

Example

```
Site-to-site tunnel:

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#security-ass
ociation inactivity-timeout 200

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#security-ass
ociation level perhost

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#security-ass
ociation lifetime kilobytes 250000

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#show context
 crypto map test 1 ipsec-isakmp
  security-association level perhost
  peer 1 ikev2 ikev2Peer1
```

```
  local-endpoint-ip 192.168.13.10
  pfs 5
  security-association lifetime kilobytes 250000
  security-association inactivity-timeout 200
  ip nat crypto
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#

Remote VPN client:

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#security-ass
ociation lifetime seconds 10000

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context
 crypto map test 2 ipsec-isakmp dynamic
  peer 1 ikev1 RemoteIKEv1Peer1
  local-endpoint-ip 157.235.204.62
  pfs 14
  security-association lifetime seconds 10000
  remote-type none
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
```

transform-set

crypto-map auto-vpn-tunnel/remote-vpn-client instance

Applies a transform set (encryption and hash algorithms) to site-to-site VPN tunnel or remote VPN client. This command allows you provide customized data protection for each crypto map can be customized with its own data protection and

peer authentication schemes.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
transform-set <TRANSFORM-SET-TAG>
```

Parameters

```
transform-set <TRANSFORM-SET-TAG>
```

transform-set <TRANSFORM-SET-TAG>	Applies a transform set. The transform set should be existing and configured • <TRANSFORM-SET-TAG> – Specify the transform set's name.

Example

```
Site-to-site VPN tunnel:

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#transform-se
t AutoVPN

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#show context
 crypto map test 1 ipsec-isakmp
```

```
  security-association level perhost
  peer 1 ikev2 ikev2Peer1
  local-endpoint-ip 192.168.13.10
  pfs 5
  security-association lifetime kilobytes 250000
  security-association inactivity-timeout 200
  transform-set AutoVPN
  ip nat crypto
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#

Remote VPN client:

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#transform-se
t RemoteVPN

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context
 crypto map test 2 ipsec-isakmp dynamic
  peer 1 ikev1 RemoteIKEv1Peer1
  local-endpoint-ip 157.235.204.62
  pfs 14
  security-association lifetime seconds 10000
  transform-set RemoteVPN
  remote-type none
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
```

use

crypto-map auto-vpn-tunnel/remote-vpn-client instance

Applies an existing and configured IP access list to the auto site-to-site VPN tunnel or remote VPN client. Based on the IP access list's settings traffic is permitted or denied across the VPN tunnel.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
use ip-access-list <IP-ACCESS-LIST-NAME>
```

Parameters

```
use ip-access-list <IP-ACCESS-LIST-NAME>
```

ip-access-list <IP-ACCESS-LIST-NAME>	Specify the IP access list name.

Example

```
Site-to-site VPN tunnel:

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)##use
ip-access-list test

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#show context
```

```
 crypto map test 1 ipsec-isakmp
  use ip-access-list test
  security-association level perhost
  peer 1 ikev2 ikev2Peer1
  local-endpoint-ip 192.168.13.10
  pfs 5
  security-association lifetime kilobytes 250000
  security-association inactivity-timeout 200
  transform-set AutoVPN
  ip nat crypto
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#

Remote VPN client:

rrfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#use
ip-access-list test1

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context
' crypto map test 2 ipsec-isakmp dynamic
  use ip-access-list test1
  peer 1 ikev1 RemoteIKEv1Peer1
  local-endpoint-ip 157.235.204.62
  pfs 14
  security-association lifetime seconds 10000
  transform-set RemoteVPN
  remote-type none
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
```

no

crypto-map auto-vpn-tunnel/remote-vpn-client instance

Removes or reverts the auto site-to-site VPN tunnel or remote VPN client settings

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no [ip|local-endpoint|modeconfig|peer|pfs|remote-type|security-association|
          transform-set|use]
```

Parameters

```
no [ip|local-endpoint|modeconfig|peer|pfs|remote-type|security-association|
transform-set|use]
```

no ip	Disables this setting to utilize IP/Port NAT on the auto site-to-site VPN tunnel
no local-endpoint-ip	Removes the configured IP as local tunnel endpoint address
no modeconfig	Resets the remote VPN client's mode config method to default (push)
no peer	Removes the configured IKEv1 or IKEv2 peer for the auto site-to-site VPN tunnel or remote VPN client

no pfs	Removes the PFS configured for this auto site-to-site VPN tunnel
no remote-type	Resets the remote VPN client type to default (XAUTH)
no security-association	Removes the VPN tunnel or remote VPN client's IPSec SA settings
no transform-set	Removes the transform set applied to the VPN tunnel or remote VPN client
no use	Removes IP access list applied to the auto site-to-site VPN tunnel or remote VPN client

Example

The following example shows the IPSec site-to-site VPN tunnel 'test' settings before the 'no' commands are executed:

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#show context
 crypto map test 1 ipsec-isakmp
  use ip-access-list test
  security-association level perhost
  peer 1 ikev2 ikev2Peer1
  local-endpoint-ip 192.168.13.10
  pfs 5
  security-association lifetime kilobytes 250000t
  security-association inactivity-timeout 200
  transform-set AutVPN
  ip nat crypto
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#no use
ip-access-list
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#no
security-association level perhost
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#no ip nat
crypto
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#no pfs
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#no
local-endpoint-ip
```

The following example shows the IPSec site-to-site VPN tunnel 'test' settings after the 'no' commands are executed:

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#show context
 crypto map test 1 ipsec-isakmp
  peer 1 ikev2 ikev2Peer1
  security-association lifetime kilobytes 250000
  security-association inactivity-timeout 200
  transform-set AutoVPN
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#
```

The following example shows the IPSec remote VPN client 'test' settings before the 'no' commands are executed:

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context
 crypto map test 2 ipsec-isakmp dynamic
  use ip-access-list test2
  peer 1 ikev1 RemoteIKEv1Peer1
  local-endpoint-ip 157.235.204.62
  pfs 14
  security-association lifetime seconds 10000
  transform-set RemoteVPN
  remote-type none
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#no use
ip-access-list
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#no peer 1
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#no
transform-set

The following example shows the IPSec remote VPN client ‘test’ settings after
the ‘no’ commands are executed:

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context
 crypto map test 2 ipsec-isakmp dynamic
  local-endpoint-ip 157.235.204.62
  pfs 14
  security-association lifetime seconds 10000
  remote-type none
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
```

crypto-map-ipsec-manual-instance

crypto-map-config-commands

To navigate to the automatic IPSec manual VPN tunnel configuration instance, use the following command:

```
In the device-config mode:
<DEVICE>(config-device-<DEVICE-MAC>)#crypto map <CRYPTO-MAP-TAG> <1-1000>
ipsec-manual

In the profile-config mode:
<DEVICE>(config-profile-<PROFILE-NAME>)#crypto map <CRYPTO-MAP-TAG> <1-1000>
          ipsec-manual

rfs4000-229D58(config-device-00-23-68-22-9D-58)#crypto map test 3 ipsec-manual
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#3)#?
Manual Crypto Map Configuration commands:
  local-endpoint-ip     Use this IP as local tunnel endpoint address, instead
                        of the interface IP (Advanced Configuration)
  mode                  Set the tunnel mode
  no                    Negate a command or set its defaults
  peer                  Set peer
  security-association  Set security association parameters
  session-key           Set security session key parameters
  use                   Set setting to use

  clrscr                Clears the display screen
  commit                Commit all changes made in this session
  do                    Run commands from Exec mode
  end                   End current mode and change to EXEC mode
  exit                  End current mode and down to previous mode
  help                  Description of the interactive help system
  revert                Revert changes
  service               Service Commands
  show                  Show running system information
  write                 Write running configuration to memory or terminal

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#3)#
```

The following table lists the IPSec manual VPN tunnel configuration commands:

Command	Description	Reference
local-endpoint-ip	Uses the configured IP as local tunnel endpoint address, instead of the interface IP (Advanced Configuration)	*page 7-622*
mode	Sets the tunnel mode	page 622
peer	Sets the peer device's IP address	*page 7-623*
security-association	Defines the lifetime (in kilobytes and/or seconds) of IPSec SAs created by a crypto map	*page 7-624*
session-key	Defines encryption and authentication keys for a crypto map	*page 7-624*
use	Uses the configured IP access list	*page 7-626*
no	Negates a command or sets its default	*page 7-626*

local-endpoint-ip

crypto-map-ipsec-manual-instance

Uses the configured IP as local tunnel endpoint address, instead of the interface IP (Advanced Configuration)

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
local-endpoint-ip <IP>
```

Parameters

```
local-endpoint-ip <IP>
```

local-endpoint-ip <IP>	Uses the configured IP as local tunnel's endpoint address • <IP> – Specify the IP address. The specified IP address must be available on the interface.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#local-endpoin
t-ip 172.16.10.3
```

mode

crypto-map-ipsec-manual-instance

Sets the crypto map tunnel mode

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
mode [transport|tunnel]
```

Parameters

```
mode [transport|tunnel]
```

mode [transport|tunnel]	Sets the mode of the tunnels for this crypto map • transport – Initiates transport mode • tunnel – Initiates tunnel mode (default setting)

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#mode
transport

rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#show context
 crypto map map1 1 ipsec-manual
  mode transport
rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#
```

peer

crypto-map-ipsec-manual-instance

Sets the peer device's IP address. This can be set for multiple remote peers. The remote peer can be an IP address.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
peer <IP>
```

Parameters

```
peer <IP>
```

peer <IP>	Enter the peer device's IP address. If not configured, it implies respond to any peer.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#peer
172.16.10.12

rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#show context
 crypto map map1 1 ipsec-manual
  peer 172.16.10.12
```

```
rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#
```

security-association

crypto-map-ipsec-manual-instance

Defines the lifetime (in kilobytes and/or seconds) of IPSec SAs created by this crypto map

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
security-association lifetime [kilobytes <500-2147483646>|seconds <120-86400>]
```

Parameters

```
security-association lifetime [kilobytes <500-2147483646>|seconds <120-86400>]
```

lifetime [kilobytes <500-2147483646>| seconds <120-86400>]	Values can be entered in both kilobytes and seconds. Which ever limit is reached first, ends the security association. • kilobytes <500-2147483646> – Defines volume based key duration. Specify a value from 500 - 2147483646 bytes. • seconds <120-86400> – Defines time based key duration. Specify the time frame from 120 - 86400 seconds.

NOTE
This command is not applicable to the ipsec-manual crypto map.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map2#2)#security-asso
ciation lifetime seconds 123

rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map2#2)#show context
 crypto map map2 2 ipsec-isakmp
  security-association lifetime seconds 123
rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map2#2)#
```

session-key

crypto-map-ipsec-manual-instance

Defines encryption and authentication keys for this crypto map

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
session-key [inbound|outbound] [ah|esp] <256-4294967295>
session-key [inbound|outbound] ah <256-4294967295> [0|2|authenticator
[md5|sha]]
          <WORD>
session-key [inbound|outbound] esp <256-4294967295> [0|2|cipher
[3des|aes|aes-192|
          aes-256|des|esp-null]] <WORD> authenticator [md5|sha] <WORD>
```

Parameters

```
session-key [inbound|outbound] ah <256-4294967295> [0|2|authenticator
[md5|sha]]
<WORD>
```

session-key [inbound|outbound]	Defines the manual inbound and outbound security association key parameters
ah <256-4294967295>	Configures *authentication header* (AH) as the security protocol for the security session • <256-4294967295> – Sets the SPI for the security association from 256 - 4294967295 The SPI (in combination with the destination IP address and security protocol) identifies the security association.

[0|2|authenticator [md5|sha] <WORD>]	Specifies the key type
	• 0 – Sets a clear text key
	• 2 – Sets an encrypted key
	• authenticator – Sets AH authenticator details
	  • md5 <WORD> – AH with MD5 authentication
	  • sha <WORD> – AH with SHA authentication
	  • <WORD> – Sets security association key value. The following key lengths (in hex characters) are required (w/o leading 0x).AH-MD5: 32, AH-SHA: 40

```
session-key [inbound|outbound] esp <256-4294967295> [0|2|cipher
[3des|aes|aes-192|aes-256|des|esp-null]] <WORD> authenticator [md5|sha] <WORD>
```

session-key [inbound|outbound]	Defines the manual inbound and outbound security association key parameters
esp <256-4294967295>	Configures *Encapsulating Security Payload*s (ESP) as the security protocol for the security session. This is the default setting. • <256-4294967295> – Sets the SPI for the security association from 256 - 4294967295 The SPI (in combination with the destination IP address and security protocol) identifies the security association.

[0|2|cipher [3des|aes|aes-192| aes-256|des|esp-null]]	• 0 – Sets a clear text key
	• 2 – Sets an encrypted key
	• cipher – Sets encryption/decryption key details
	  • 3des – ESP with 3DES encryption
	  • aes – ESP with AES encryption
	  • aes-192 – ESP with AES-192 encryption
	  • aes-256 – ESP with AES-256 encryption
	  • des – ESP with DES encryption
	  • esp-null – ESP with no encryption
	  • authenticator – Specify ESP authenticator details
	  • md5 <WORD> – ESP with MD5 authentication
	  • sha <WORD> – ESP with SHA authentication
	  • <WORD> – Sets security association key value. The following key lengths (in hex characters) are required (w/o leading 0x).AH-MD5: 32, AH-SHA: 40

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#session-key
inbound esp 273 cipher esp-null authenticator sha 58768979

rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#show context
 crypto map map1 1 ipsec-manual
  peer 172.16.10.2
  mode transport
  session-key inbound esp 273 0 cipher esp-null authenticator sha 58768979
rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#
```

use

crypto-map-ipsec-manual-instance

Uses the configured IP access list

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
use ip-access-list <IP-ACCESS-LIST-NAME>
```

Parameters

```
use ip-access-list <IP-ACCESS-LIST-NAME>
```

ip-access-list <IP-ACCESS-LIST-NAME>	Specify the IP access list name.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#use
ip-access-list test

rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#show context
 crypto map map1 1 ipsec-manual
  use ip-access-list test
  peer 172.16.10.12
  mode transport
  session-key inbound esp 273 0 cipher esp-null authenticator sha 5876897
rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#
```

no

crypto-map-ipsec-manual-instance

Negates a command or reverts settings to their default

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no [local-endpoint-ip|mode|peer|security-association|session-key|use]
```

Parameters

```
no [local-endpoint-ip|mode|peer|security-association|session-key|use]
```

no local-endpoint-ip	Deletes the local IP address
no mode	Resets the tunnelling mode to default (Tunnel)
no peer	Deletes the remote peer settings
no security-association	Deletes the security association parameters
no session-key	Deletes the session key parameters
no use	Resets the IP access list parameters values

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#show context
 crypto map map1 1 ipsec-manual
  use ip-access-list test
  peer 172.16.10.12
  mode transport
  session-key inbound esp 273 0 cipher esp-null authenticator sha 5876897
rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#

rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#no use
ip-access-list
rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#no peer
rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#no mode

rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#show context
 crypto map map1 1 ipsec-manual
  session-key inbound esp 273 0 cipher esp-null authenticator sha 58768979
rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#
```

crypto-remote-vpn-client commands

crypto

This section documents the IKEV2 remote VPN client configuration settings. Use this command to define the server resources used to secure (authenticate) a remote VPN connection with a target peer.

Use the profile-config instance to configure remote VPN client settings. To navigate to the remote-vpn-client configuration instance, use the following commands:

```
<DEVICE>(config)#profile <DEVICE-TYPE> <PROFILE-NAME>
<DEVICE>(config-profile-<PROFILE-NAME>)#crypto remote-vpn-client
<DEVICE>(config-profile-<PROFILE-NAME>-crypto-ikev2-remote-vpn-client)#
```

NOTE
To configure remote VPN client settings on a device, on the device's configuration mode, use the *crypto > remote-vpn-client* command.
For example: `rfs4000-229D58(config-device-00-23-68-22-9D-58)#crypto remote-vpn-client`

NOTE
The following configuration enables a access point to adopt to a controller over the remote VPN link:
On a profile: `rfs4000-229D58(config-profile-testBrocade Mobility RFS4000)#controller host <HOST-IP> remote-vpn-client`

On a device: `rfs4000-229D58(config-00-23-68-22-9D-58)#controller host <HOST-IP> remote-vpn-client`

```
rfs4000-229D58(config)#profile rfs4000 testBrocade Mobility RFS4000
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000)#

rfs4000-229D58(config-profile-testBrocade Mobility RFS4000)#crypto
remote-vpn-client
rfs4000-229D58(config-profile-testBrocade Mobility
RFS4000-crypto-ikev2-remote-vpn-client)#?
Crypto IKEV2 Remote Vpn Client Config commands:
  no              Negate a command or set its defaults
  peer            Add a remote peer
  shutdown        Disable remote vpn client
  transform-set   Specify IPSec transform to use

  clrscr          Clears the display screen
  commit          Commit all changes made in this session
  do              Run commands from Exec mode
  end             End current mode and change to EXEC mode
  exit            End current mode and down to previous mode
  help            Description of the interactive help system
  revert          Revert changes
  service         Service Commands
  show            Show running system information
  write           Write running configuration to memory or terminal

rfs4000-229D58(config-profile-testBrocade Mobility
RFS4000-crypto-ikev2-remote-vpn-client)#
```

The following table summarizes crypto remote VPN client configuration mode commands.

Command	Description	Reference
peer	Adds a remote IKEv2 peer	page 628
shutdown	Disables the remote VPN client	page 629
transform-set	Associates an existing IPSec transform set with this remote VPN client	page 630
no	Removes the remote VPN client settings	page 631

peer

crypto-remote-vpn-client commands

Adds a new remote peer. A maximum of three (3) peers can be added to support redundancy.

IKEv2 uses an initial handshake in which VPN peers negotiate cryptographic algorithms, mutually authenticate, and establish a session key, creating an IKE-SA. Additionally, a first IPsec SA is established during the initial SA creation. All IKEv2 messages are request/response pairs. It is the responsibility of the side sending the request to retransmit if it does not receive a timely response.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
peer <1-3> ikev2 <IKEV2-PEER-NAME>
```

Parameters

```
peer <1-3> ikev2 <IKEV2-PEER-NAME>
```

peer <1-3>	Adds a IKEv2 peer. You can add multiple peers to achieve redundancy • <1-3> – Specify a priority level for the peer from 1 - 3 (1 = primary, 2 and 3 = redundant).
ikev2 <IKEV2-PEER-NAME>	Specifies a name for this IKEv2 peer.

Example

```
rfs4000-229D58(config-profile-testBrocade Mobility
RFS4000-crypto-ikev2-remote-vpn-client)#peer
1 ikev2 ikev2Peer1

rfs4000-229D58(config-profile-testBrocade Mobility
RFS4000-crypto-ikev2-remote-vpn-client)#peer 2
 ikev2 ikev2Peer2

rfs4000-229D58(config-profile-testBrocade Mobility
RFS4000-crypto-ikev2-remote-vpn-client)#show context
 crypto remote-vpn-client
  peer 1 ikev2 ikev2Peer1
  peer 2 ikev2 ikev2Peer2
rfs4000-229D58(config-profile-testBrocade Mobility
RFS4000-crypto-ikev2-remote-vpn-client)#
```

shutdown

crypto-remote-vpn-client commands

Disables remote-vpn-client on this profile or device. Remote VPN client feature is disabled by default.

To enable remote VPN client, use the *no* > *shutdown* command.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
shutdown
```

Parameters

None

Example

```
rfs4000-229D58(config-profile-testBrocade Mobility
RFS4000-crypto-ikev2-remote-vpn-client)#
shutdown
rfs4000-229D58(config-profile-testBrocade Mobility
RFS4000-crypto-ikev2-remote-vpn-client)#
```

transform-set

crypto-remote-vpn-client commands

Specifies the IPSec Transform to use with the remote VPN client. A transform set is a combination of security protocols, algorithms, and other settings applied to IPSec protected client traffic.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
transform-set <IPSEC-XFORM-TAG>
```

Parameters

```
transform-set <IPSEC-XFORM-TAG>
```

transform-set <IPSEC-XFORM-TAG>	Associates an IPSec Transform (should be existing and configured) set with this remote VPN client. To configure a transform-set, use the *crypto* > *ipsec* > *transform-set* command in the profile or device configuration mode.

Example

```
rfs4000-229D58(config-profile-testBrocade Mobility
RFS4000-crypto-ikev2-remote-vpn-client)#trans
form-set TransformSet1

rfs4000-229D58(config-profile-testBrocade Mobility
RFS4000-crypto-ikev2-remote-vpn-client)#show
context
 crypto remote-vpn-client
  peer 1 ikev2 ikev2Peer1
  transform-set TransformSet1
```

```
rfs4000-229D58(config-profile-testBrocade Mobility
RFS4000-crypto-ikev2-remote-vpn-client)#
```

no

crypto-remote-vpn-client commands

Removes the remote VPN client settings

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no [peer <1-3>|shutdown|transform-set]
```

Parameters

```
no [peer <1-3>|shutdown|transform-set]
```

no peer <1-3>	Removes the remote IKEv2 peer with the specified priority
no shutdown	Enables remote VPN client
transform-set	Disassociates the transform set attached with this remote VPN client

Example

```
rfs4000-229D58(config-profile-testBrocade Mobility
RFS4000-crypto-ikev2-remote-vpn-client)#)#show context
 crypto remote-vpn-client
  peer 1 ikev2 peer5
rfs4000-229D58(config-profile-testBrocade Mobility
RFS4000-crypto-ikev2-remote-vpn-client)#

rfs4000-229D58(config-profile-testBrocade Mobility
RFS4000-crypto-ikev2-remote-vpn-client)##no peer 1
rfs4000-229D58(config-profile-testBrocade Mobility
RFS4000-crypto-ikev2-remote-vpn-client)#

rfs4000-229D58(config-profile-testBrocade Mobility
RFS4000-crypto-ikev2-remote-vpn-client)#show context
 crypto remote-vpn-client
rfs4000-229D58(config-profile-testBrocade Mobility
RFS4000-crypto-ikev2-remote-vpn-client)#
```

device-upgrade

Profile Config Commands

Configures device firmware upgrade settings on this profile. Access points, wireless controllers, and service platforms using this profile automatically upgrade firmware on adopted devices.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
device-upgrade [add-auto|auto|count|persist-images]

device-upgrade add-auto
[(ap621|ap622|br650|br6511|ap6521|br1220|ap6532|ap6562|
          br71xx|br81xx|ap82xx|rfs4000|rfs6000|rfs7000)]

device-upgrade auto
{(ap621|ap622|br650|br6511|ap6521|br1220|ap6532|ap6562|br71xx|
          br81xx|ap82xx|rfs4000|rfs6000|rfs7000)}

device-upgrade count <1-20>

device-upgrade persist-images
```

Parameters

```
device-upgrade add-auto
[(ap621|ap622|br650|br6511|ap6521|br1220|ap6532|ap6562|
br71xx|br81xx|ap82xx|rfs4000|rfs6000|rfs7000)]
```

device-upgrade add-auto	Configures a list of devices types for automatic firmware upgrade This command specifies the types of devices that can be automatically upgraded (if enabled). To enable automatic device firmware upgrade, use the 'auto' command. When enabled, access points, wireless controllers, and service platforms, using this profile, will automatically upgrade firmware on adopted devices that match the specified device types.
[br650|br6511|ap6521|br1220| ap6532|ap6562|br71xx| br81xx|ap82xx|rfs4000| rfs6000|rfs7000]	Adds selected devices to the device type list • Brocade Mobility 650 Access Point – Adds Brocade Mobility 650 Access Point device to the auto device type list • Brocade Mobility 6511 Access Point– Adds Brocade Mobility 6511 Access Point device to the auto device type list • Brocade Mobility 1220 Access Point – Adds Brocade Mobility 1220 Access Point device to the auto device type list • Brocade Mobility 71XX Access Point – Adds Brocade Mobility 71XX Access Point device to the auto device type list • Brocade Mobility 1240 Access Point – Adds Brocade Mobility 1240 Access Point device to the auto device type list • Brocade Mobility RFS4000 – Adds Brocade Mobility RFS4000 device to the auto device type list • Brocade Mobility RFS6000 – Adds Brocade Mobility RFS6000 device to the auto device type list • Brocade Mobility RFS7000 – Adds Brocade Mobility RFS7000 device to the auto device type list Multiple device types can be added to the add-auto list

```
device-upgrade auto
{(ap621|ap622|br650|br6511|ap6521|br1220|ap6532|ap6562|br71xx|
br81xx|ap82xx|rfs4000|rfs6000|rfs7000)}
```

device-upgrade auto	Enables automatic firmware upgrade on specified device types. When used along with the add-auto command, the auto command allows access points, wireless controllers, and service platforms to automatically upgrade firmware on adopted devices matching the specified device types.
{(ap621|ap622|br650|br6511|ap6521|br1220|ap6532|ap6562|br71xx|br81xx|ap82xx|rfs4000|rfs6000|rfs7000)}	Selects the device types for automatic firmware upgrade • Brocade Mobility 650 Access Point – Optional. Enables automatic Brocade Mobility 650 Access Point firmware image upgrade • Brocade Mobility 6511 Access Point – Optional. Enables automatic Brocade Mobility 6511 Access Point firmware image upgrade • Brocade Mobility 1220 Access Point – Optional. Enables automatic Brocade Mobility 1220 Access Point firmware image upgrade • Brocade Mobility 71XX Access Point – Optional. Enables automatic Brocade Mobility 71XX Access Point firmware image upgrade • Brocade Mobility 1240 Access Point – Optional. Enables automatic Brocade Mobility 1240 Access Point firmware image upgrade • Brocade Mobility RFS4000 – Optional. Enables automatic Brocade Mobility RFS4000 firmware image upgrade • Brocade Mobility RFS6000 – Optional. Enables automatic Brocade Mobility RFS6000 firmware image upgrade • Brocade Mobility RFS7000 – Optional. Enables automatic Brocade Mobility RFS7000 firmware image upgrade Multiple device types can be added to the auto list

```
device-upgrade count <1-20>
```

device-upgrade count <1-20>	Configures the maximum number of concurrent upgrades possible • <1-20> – specify a value from 1 - 20.

```
device-upgrade persist-images
```

device-upgrade	Configures parameters for automatic firmware upgrade of adopted devices. Use this command to select the device types and the maximum number of concurrent upgrades.
images	Enables RF Domain manager to retain AP firmware image after upgrade, subject to availability of space By default this feature is enabled for wireless controllers and disabled for access points.

Example

```
rfs4000-229D58(config-profile-default-rfs4000)#device-upgrade auto br71xx
rfs4000-229D58(config-profile-default-rfs4000)#

rfs4000-229D58config-profile-default-rfs4000)#show context
profile rfs4000 default-rfs4000
 autoinstall configuration
 autoinstall firmware
 device-upgrade auto br71xx
 device-upgrade persist-br-image
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 interface radio1
 interface radio2
```

```
 interface up1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
--More--
rfs4000-229D58(config-profile-default-rfs4000)#
```

Related Commands:

no	Removes device firmware upgrade settings on this profile
Chapter 3, device-upgrade	Displays device upgrade details

dot1x

Profile Config Commands

Configures 802.1x standard authentication controls

Dot1x (or 802.1x) is an IEEE standard for network authentication. It enables media-level (layer 2) access control, providing the capability to permit or deny connectivity based on user or device identity. Dot1x allows port-based access using authentication. An dot1x enabled port can be dynamically enabled or disabled depending on user identity or device connection.

Devices supporting dot1x allow the automatic provision and connection to the wireless network without launching a Web browser at login. When within range of a dot1x network, a device automatically connects and authenticates without needing to manually login.

Before authentication, the endpoint is unknown, and traffic is blocked. Upon authentication, the endpoint is known and traffic is allowed. The controller or service platform uses source MAC filtering to ensure only the authenticated endpoint is allowed to send traffic.

Supported in the following platforms:

- Access Points — Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
dot1x [guest-vlan|system-auth-control|use]

dot1x system-auth-control
dot1x guest-vlan supplicant
dot1x use aaa-policy <AAA-POLICY-NAME>
```

Parameters

```
dot1x system-auth-control
```

system-auth-control	Enables or disables system auth control. Enables/disables dot1x authorization globally for the controller. This feature is disabled by default.

dot1x guest-vlan supplicant	
guest-vlan	Configures guest VLAN and supplicant behavior This feature is disabled by default.
supplicant	Allows 802.1x capable supplicant to enter guest VLAN. When enabled, this is the VLAN that supplicant's traffic is bridged on.

dot1x use aaa-policy <AAA-POLICY-NAME>	
use aaa-policy <AAA-POLICY-NAME>	Associates a specified 802.1x AAA policy with this access point profile • <AAA-POLICY-NAME> – Specify the AAA policy name. Once specified, this AAA policy is utilized for authenticating user requests.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#dot1x use aaa-policy test

rfs7000-37FABE(config-profile-default-rfs7000)#dot1x system-auth-control

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
 ..................................................
  interface pppoe1
 use firewall-policy default
service pm sys-restart
 router ospf
 dot1x system-auth-control
 dot1x use aaa-policy test
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Disables or reverts settings to their default

dscp-mapping

Profile Config Commands

Configures IP *Differentiated Services Code Point* (DSCP) to 802.1p priority mapping for untagged frames

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
dscp-mapping <WORD> priority <0-7>
```

Parameters

```
dscp-mapping <word> priority <0-7>
```

<WORD>	Specifies the DSCP value of a received IP packet. This could be a single value or a list. For example, 10-20, 25, 30-35.
priority <0-7>	Specifies the 802.1p priority to use for a packet if untagged. The priority is set on a scale of 0 - 7.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#dscp-mapping 20 priority 7

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 dscp-mapping 20 priority 7
 no autoinstall configuration
 no autoinstall firmware
 crypto isakmp policy default
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 interface me1
 interface ge1
 ip dhcp trust
 qos trust dscp
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Disables or reverts settings to their default

email-notification

Profile Config Commands

Configures e-mail notification settings

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
email-notification [host|recipient]

email-notification recipient <RECIPIENT-NAME>

email-notification host <SMTP-SERVER-IP> sender <SENDER-EMAIL> {port|username}

email-notification host <SMTP-SERVER-IP> sender <SENDER-EMAIL> {port
<1-65535>}
          {username <SMTP-USERNAME>} [password [2 <WORD>|<WORD>]]
```

```
email-notification host <SMTP-SERVER-IP> sender <SENDER-EMAIL>
          {username <SMTP-USERNAME>} [password [2 <WORD>|<WORD>]] {port
<1-65535>}
```

Parameters

```
email-notification recipient <RECIPIENT-EMAIL>
```

recipient <RECIPIENT-EMAIL>	Defines the recipient's e-mail address. A maximum of 6 (six) e-mail addresses can the configured. • <RECIPIENT-EMAIL> – Specify the recipient's e-mail address (should not exceed 64 characters in length).

```
email-notification host <SMTP-SERVER-IP> sender <SENDER-EMAIL> {port
<1-65535>}{username <SMTP-USERNAME>} [password [2 <WORD>|<WORD>]]
```

host <SMTP-SERVER-IP>	Configures the host SMTP server • <SMTP-SERVER-IP> – Specify the SMTP server's IP address.
sender <SENDER-EMAIL>	Defines the sender's e-mail address • <SENDER-EMAIL> – Specify the sender's e-mail address (should not exceed 64 characters in length).
port <1-65535>	Optional. Configures the SMTP server port • <1-65535> – Specify the port from 1 - 65535.
username <SMTP-USERNAME>	Optional. Configures the SMTP username • <SMTP-USERNAME> – Specify the SMTP username (should not exceed 64 characters in length).
password [2 <WORD>|<WORD>]	Configures the SMTP server password • 2 <WORD> – Configures an encrypted password • <WORD> – Specify the password (should not exceed 127 characters in length).

```
email-notification host <SMTP-SERVER-IP> sender <SENDER-EMAIL>
{username <SMTP-USERNAME>} [password [2 <WORD>|<WORD>] {port <1-65535>}
```

host <SMTP-SERVER-IP>	Configures the host SMTP server • <SMTP-SERVER-IP> – Specify the IP address of the SMTP server.
sender <SENDER-EMAIL>	Defines sender's e-mail address • <SENDER-EMAIL> – Specify sender's e-mail address.
username <SMTP-USERNAME>	Optional. Configures the SMTP username • <SMTP-USERNAME> – Specify the SMTP username.
password [2 <WORD>|<WORD>]	Configures the SMTP server password • 2 <WORD> – Configures an encrypted password • <WORD> – Specify the password.
port <1-65535>	Optional. Configures the SMTP server port • <1-65535> – Specify the port from 1 - 65535.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#email-notification recipient
test@motorolasoultions.com

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 dscp-mapping 20 priority 7
 no autoinstall configuration
 no autoinstall firmware
 ..........................................................
 interface ge4
  ip dhcp trust
```

```
 qos trust dscp
 qos trust 802.1p
use firewall-policy default
email-notification recipient test@motorolasolutions.com
service pm sys-restart
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Disables or reverts settings to their default

enforce-version

Profile Config Commands

Enables checking of a device's firmware version before attempting adoption or clustering

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
enforce-version [adoption|cluster] [full|major|minor|none|strict]
```

Parameters

```
enforce-version [adoption|cluster] [full|major|minor|none|strict]
```

adoption	Verifies firmware versions before adopting
cluster	Verifies firmware versions before clustering
full	Allows adoption or clustering when the first four octets of the firmware versions match (for example 5.4.2.0)
major	Allows adoption or clustering when the first two octets of the firmware versions match (for example 5.4)
minor	Allows adoption or clustering when the first three octets of the firmware versions match (for example 5.4.2)
none	Allows adoption or clustering between any firmware versions
strict	Allows adoption or clustering only when firmware versions exactly match (for example 5.4.2.0-006D)

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#enforce-version cluster full

rfs7000-37FABE(config-profile-default-rfs7000)#enforce-version adoption major

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 bridge vlan 1
  bridging-mode isolated-tunnel

 ..................................................
 interface pppoe1
```

```
 use firewall-policy default
enforce-version adoption major
 enforce-version cluster full
 service pm sys-restart
 router ospf
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Disables or reverts settings to their default

environmental-sensor

Profile Config Commands

Configures the environmental sensor settings

A Brocade Mobility 1240 Access Point sensor module is a USB environmental sensor extension to a Brocade Mobility 1240 Access Point model access point. It provides a variety of sensing mechanisms, allowing the monitoring and reporting of the Brocade Mobility 1240 Access Point's radio coverage area.

Supported in the following platforms:

- Access Points — Brocade Mobility 1240 Access Point

Syntax:

```
environmental-sensor [humidity|light|motion|polling-interval|temperature]

environmental-sensor [humidity|motion|polling-interval <1-100>|temperature]

environmental-sensor light {holdtime|radio-shutdown|threshold}
environmental-sensor light {holdtime <2-201>|radio-shutdown
[all|radio-1|radio-2]}
environmental-sensor light {threshold [high <100-10000>|low <0-1000>]}
```

Parameters

```
environmental-sensor [humidity|motion|polling-interval <1-100>|temperature]
```

environmental-sensor	Configures environmental sensor settings on this profile
humidity	Enables (turns on) humidity sensors. This setting is enabled by default.
motion	Enables (turns on) motion sensors.This setting is enabled by default.
polling-interval <1-100>	Configures polling interval, in seconds, on all sensors. This is the interval after which the sensor module polls its environment to assess the various parameters, such as light intensity. • <1-100> – Specify a value from 1 - 100 seconds. The default is 11 seconds.
temperature	Enables (turns on) temperature sensors. This setting is enabled by default.

```
environmental-sensor light {holdtime <2-201>|radio-shutdown
[all|radio-1|radio-2]}
```

environmental-sensor	Configures environmental sensor settings on this profile
light	Enables (turns on) light sensors and specifies its settings When enabled, the sensor module polls the environment to determine the light intensity. Based on the reading, the system determines whether the Brocade Mobility 1240 Access Point's deployment location has lights on or off. Light intensity also helps determine whether the access point's deployment location is currently populated with clients.
holdtime <2-201>	Optional. Configures a holdtime, in seconds, for the light sensor • <2-201> – Specify a value from 2 - 201 seconds.
radio-shutdown [all|radio1|radio2]	Optional. Shuts down the sensor's radios • all – Shuts down all radios • radio1 – Shuts down radio 1 • radio2 – Shuts down radio 2 Brocade Mobility 1240 Access Point's using this profile have their radios shut down, when the radio's power falls below the specified threshold.

```
environmental-sensor light {threshold [high <100-10000>|low <0-1000>]}
```

environmental-sensor	Configures environmental sensor settings on this profile
light	Enables (turns on) light sensors and specifies its settings
threshold	Optional. Configures the upper and lower thresholds for the amount of light in the environment
high <100-10000>	Specifies the upper threshold from 100 - 10000 lumens. This value determines whether lighting is on in the AP8132's deployment location. The default is 500 lux. The light sensor triggers an event if the amount of light exceeds the specified value.
low <0-1000>	Specifies the lower threshold from 0 - 1000 lumens. This value determines whether lighting is off in the Brocade Mobility 1240 Access Point's deployment location. The default is 100 lux. The light sensor triggers an event if the amount of light drops below the specified value.

Example

```
rfs4000-229D58(config-profile-testBrocade Mobility
RFS4000)#environmental-sensor humidity

rfs4000-229D58(config-profile-testBrocade Mobility
RFS4000)#environmental-sensor polling-interval 60

rfs4000-229D58(config-profile-testBrocade Mobility
RFS4000)#environmental-sensor light radio-shutdown all

rfs4000-229D58(config-profile-testBrocade Mobility
RFS4000)#environmental-sensor light threshold high 300

rfs4000-229D58(config-profile-testBrocade Mobility
RFS4000)#environmental-sensor light threshold low 100

rfs4000-229D58(config-profile-testBrocade Mobility RFS4000)#show context
profile rfs4000 testBrocade Mobility RFS4000
 bridge vlan 1
  tunnel-over-level2
  ip igmp snooping
  ip igmp snooping querier
 environmental-sensor polling-interval 60
 environmental-sensor light threshold high 300
 environmental-sensor light threshold low 100
```

```
 environmental-sensor light radio-shutdown all
 no autoinstall configuration
 no autoinstall firmware
 device-upgrade persist-images
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
--More--
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000)#
```

Related Commands:

no	Removes the environmental sensor's settings

events

Profile Config Commands

Displays system event messages

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
events [forward on|on]
```

Parameters

```
event [forward on|on]
```

forward on	Forwards system event messages to the wireless controller, service platform, or cluster members. This feature is enabled by default. • on – Enables forwarding of system events
on	Generates system events. This feature is enabled by default.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#events forward on
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Disables or reverts settings to their default

export

Profile Config Commands

Enables export of startup.log file after every boot

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
export startup-log [max-retries|retry-interval|url]
export startup-log [max-retries <2-65535>|retry-interval <30-86400>|url <URL>]
```

Parameters

```
export startup-log [max-retries <2-65535>|retry-interval <30-86400>|url <URL>]
```

export startup-log	Enables export of the startup.log file after every boot
max-retries <2-65535>	Configures the maximum number of retries in case the export process fails • <2-65535> – Specify a value from 2 - 65535.
retry-interval <30-86400>	Configures the interval between two consecutive retries • <30-86400> – Specify a value from 30 - 86400 seconds.
url <URL>	Configures the destination URL in the following format: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#export startup-log max-retries
10
 retry-interval 30 url test@motorolasolutions.com

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 bridge vlan 1
 ..................................................
  qos trust dscp
  qos trust 802.1p
 interface ge4
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface pppoe1
 use firewall-policy default
 export startup-log max-retries 10 retry-interval 30 url
test@motorolasolutions.com
service pm sys-restart
 router ospf
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Disables export of startup.log file

floor

Profile Config Commands

Sets the floor name where the system is located

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
floor <WORD> {<1-4094>}
```

Parameters

```
floor <WORD> {<1-4094>}
```

floor <WORD> {<1-4094>}	Sets the floor name where the system is located • <WORD> – Specify the floor name. • <1-4094> – Optional. Configures the floor number from 1 - 4094.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#floor fifth
rfs7000-37FABE(config-profile-default-rfs7000)#

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 bridge vlan 1
  ip igmp snooping
  ip igmp snooping querier
 area Ecospace
 floor fifth
 autoinstall configuration
 autoinstall firmware
--More--
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Resets the configured floor name and number

gre

Profile Config Commands

Command	Description	Reference
gre	Enables GRE tunneling on a profile/device This command also creates a GRE tunnel and enters its configuration mode. Use this command to modify an existing GRE tunnel's settings.	page 644
gre-config-instance	Summarizes GRE tunnel configuration mode commands	page 646

gre

gre

Enables *Generic Routing Encapsulation* (GRE) tunneling on this profile, and creates a new GRE tunnel or modifies an existing GRE tunnel.

The GRE protocol allows encapsulation of one protocol over another. It is a tunneling protocol that transports any layer 3 protocol over an IP network. When enabled, a payload packet is first encapsulated in the GRE protocol. The GRE encapsulated payload is then encapsulated in another IP packet before being forwarded to the destination.

GRE tunneling can be configured to bridge Ethernet packets between WLANs and a remote WLAN gateway over an IPv4 GRE tunnel. The tunneling of 802.3 packets using GRE is an alternative to MiNT or L2TPv3. Related features like ACLs for extended VLANs are still available using layer 2 tunneling over GRE.

Using GRE, access points map one or more VLANs to a tunnel. The remote end point is a user-configured WLAN gateway IP address, with an optional secondary IP address should connectivity to the primary GRE peer be lost. VLAN traffic is expected in both directions in the GRE tunnel. A WLAN mapped to these VLANs can be either open or secure. Secure WLANs require authentication to a remote RADIUS server available within your deployment using standard RADIUS protocols. Access Points can reach both the GRE peer as well as the RADIUS server using IPv4.

NOTE
Only one GRE tunnel can be created for every profile.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
gre tunnel <GRE-TUNNEL-NAME>
```

Parameters

```
gre tunnel <GRE-TUNNEL-NAME>
```

gre tunnel <GRE-TUNNEL-NAME>	Creates a new GRE tunnel or modifies an existing GRE tunnel • <GRE-TUNNEL-NAME> – If creating a new tunnel, specify a unique name for it. If modifying an existing tunnel, specify its name.

Example

```
rfs4000-229D58(config-profile testBrocade Mobility
RFS4000-gre-tunnel-testGREtunnel)#?
GRE Tunnel Mode commands:
  dscp           Differentiated Services Code Point
  failover       Gre tunnel failover
  native         Native trunking characteristics
  no             Negate a command or set its defaults
  peer           GRE peer
  tunneled-vlan  VLANs to tunnel

  clrscr         Clears the display screen
  commit         Commit all changes made in this session
  end            End current mode and change to EXEC mode
  exit           End current mode and down to previous mode
  help           Description of the interactive help system
  revert         Revert changes
  service        Service Commands
  show           Show running system information
  write          Write running configuration to memory or terminal

rfs4000-229D58(config-profile testBrocade Mobility
RFS4000-gre-tunnel-testGREtunnel)#

rfs4000-229D58(config-profile testBrocade Mobility
RFS4000-gre-tunnel-testGREtunnel)#peer 1 ip 192.168.13.8
rfs4000-229D58(config-profile testBrocade Mobility
RFS4000-gre-tunnel-testGREtunnel)#peer 2 ip 192.168.13.10

rfs4000-229D58(config-profile testBrocade Mobility
RFS4000-gre-tunnel-testGREtunnel)#show context
 gre tunnel testGREtunnel
  peer 1 ip 192.168.13.8
  peer 2 ip 192.168.13.10
rfs4000-229D58(config-profile testBrocade Mobility
RFS4000-gre-tunnel-testGREtunnel)#

rfs4000-229D58(config-profile-testBrocade Mobility RFS4000)#show context
profile rfs4000 testBrocade Mobility RFS4000
 bridge vlan 1
  tunnel-over-level2
  ip igmp snooping
  ip igmp snooping querier
.....................................................................................
.....
 use firewall-policy default
 service pm sys-restart
 router ospf
 gre tunnel testGREtunnel
  peer 1 ip 192.168.13.8
  peer 2 ip 192.168.13.10
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000)#
```

Related Commands:

no	Disables GRE tunneling on this profile

gre-config-instance

gre

The following table summarizes GRE tunnel configuration mode commands.

Command	Description	Reference
dscp	Sets the GRE tunnel's *Differentiated Services Code Point* (DSCP) / 802.1q priority value	page 646
failover	Enables periodic pinging of the primary gateway to assess its availability, in case it is unreachable	page 647
native	Configures native trunking settings for this GRE tunnel	page 648
no	Removes the GRE tunnel settings based on the parameters passed	page 649
peer	Configures the GRE tunnel's end-point peers	page 650
tunneled-vlan	Defines the VLAN that connected clients use to route GRE-tunneled traffic within their respective WLANs	page 651

dscp

gre-config-instance

Sets the GRE tunnel's DSCP / 802.1q priority value from encapsulated packets to the outer packet IPv4 header.

This option is disabled by default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
dscp [<0-63>|reflect]
```

Parameters

```
dscp [<0-63>|reflect]
```

dscp <0-63>	Specifies the DSCP 802.1q priority value for outer packets from 0 - 63. The default is 1.
dscp reflect	Copies the DSCP 802.1q value from inner packets

Example

```
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#dscp
20
```

```
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#show
co
ntext
 gre tunnel testGRETunnel
  dscp 20
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#

The following example configures a GRE tunnel on a profile:

nx4500-5CFA2B(config-profile testNX45XX-gre-tunnel-testGRETunnel)#dscp 20

nx4500-5CFA2B(config-profile testNX45XX-gre-tunnel-testGRETunnel)#show
context
 gre tunnel testGRETunnel
  dscp 20
nx4500-5CFA2B(config-profile testNX45XX-gre-tunnel-testGRETunnel)#
```

Related Commands:

no	Removes the GRE tunnel settings based on the parameters passed

failover

gre-config-instance

Enables periodic pinging of the primary gateway to assess its availability. When enabled, the system continues pinging, an unreachable gateway, for a specified number of times and at the specified interval.

This option is disabled by default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
failover interval <0-86400> retry <0-10>
```

Parameters

```
failover interval <0-86400> retry <0-10>
```

failover interval <0-86400> retry <0-10>	Specifies the interval, in seconds, between two successive pings to the primary gateway. If the primary gateway is unreachable, the system pings it at intervals specified here. • <0-86400> – Specify a value from 0 - 86400 seconds. • retry – Specifies the maximum number attempts made to ping the primary gateway before the session is terminated. • <0-10> – Specify a value from 0 - 10.

Example

```
rfs4000-229D58(config-device
00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#failover interval 200 retry 5
```

```
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#show
context
 gre tunnel testGRETunnel
  dscp 20
  failover interval 200 retry 5
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#
```

Related Commands:

no	Removes the GRE tunnel settings based on the parameters passed

native

gre-config-instance

Configures native trunking settings for this GRE tunnel

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
native [tagged|vlan <1-4094>]
```

Parameters

```
native [tagged|vlan <1-4094>]
```

native tagged	Tags the native VLAN The IEEE 802.1Q specification is supported for tagging frames and coordinating VLANs between devices. IEEE 802.1Q adds four bytes to each frame identifying the VLAN ID for upstream devices that the frame belongs. If the upstream Ethernet device does not support IEEE 802.1Q tagging, it does not interpret the tagged frames. When VLAN tagging is required between devices, both devices must support tagging and be configured to accept tagged VLANs. When a frame is tagged, the 12 bit frame VLAN ID is added to the 802.1Q header so upstream Ethernet devices know which VLAN ID the frame belongs to. The device reads the 12 bit VLAN ID and forwards the frame to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream device classifies the frame using the default or native VLAN assigned to the Trunk port. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. This feature is disabled by default.
native vlan <1-4094>	Specifies a numerical VLAN ID (1 - 4094) for the native VLAN The native VLAN allows an Ethernet device to associate untagged frames to a VLAN, when no 802.1q frame is included in the frame. Additionally, the native VLAN is the VLAN untagged traffic is directed over when using a port in trunk mode.

Example

```
rfs4000-229D58(config-device
00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#native
tagged

rfs4000-229D58(config-device
00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#native
```

```
vlan 1

rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#show
co
ntext
 gre tunnel testGRETunnel
  native tagged
  dscp 20
  failover interval 200 retry 5
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#
```

Related Commands:

no	Removes the GRE tunnel settings based on the parameters passed

no

gre-config-instance

Removes the GRE tunnel settings based on the parameters passed

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no [dscp|failover|native|peer|tunneled-vlan]
```

Parameters

```
no [dscp|failover|native|peer|tunneled-vlan]
```

no <PARAMETER>	Removes the GRE tunnel's settings based on the parameters passed

Example

```
The following example shows the GRE tunnel 'testGRETunnel' settings before the
no commands are executed:

rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#show
context
 gre tunnel testGRETunnel
  peer 1 ip 192.168.13.6
  native vlan 1
  tunneled-vlan 1,10
  native tagged
  dscp 20
  failover interval 200 retry 5
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#

rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#no
dscp
```

```
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#no
native vlan

rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#no
tunneled-vlan

rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#no
failover

The following example shows the GRE tunnel 'testGRETunnel' settings after the
no commands are executed:

rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#show
context
 gre tunnel testGRETunnel
  peer 1 ip 192.168.13.6
  native tagged
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#
```

Related Commands:

dscp	Sets the GRE tunnel's DSCP / 802.1q priority value
failover	Enables periodic pinging of the primary gateway to assess its availability, in case it is unreachable
native	Configures native trunking settings for this GRE tunnel
peer	Configures the GRE tunnel's end-point peers
tunneled-vlan	Defines the VLAN that connected clients use to route GRE tunneled traffic within their respective WLANs

peer

gre-config-instance

Adds the GRE tunnel's end-point peers. A maximum of two peers, representing the tunnel's end points, can be added for each GRE tunnel.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
peer <1-2> ip <IP>
```

Parameters

```
peer <1-2> ip <IP>
```

peer <1-2> ip <IP>	Configures the tunnel's end-point peers • <1-2> – Specify a numeric index for each peer to help differentiate the tunnel end points. • ip – Specifies the IP address of the added GRE peer to serve as a network address identifier. • <IP> – Specify the peer's IP address.

Example

```
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#peer
1
ip 192.168.13.6

rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#show
co
ntext
 gre tunnel testGRETunnel
  peer 1 ip 192.168.13.6
  native tagged
  dscp 20
  failover interval 200 retry 5
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#
```

Related Commands:

no	Removes the GRE tunnel settings based on the parameters passed

tunneled-vlan

gre-config-instance

Defines the VLAN that connected clients use to route GRE tunneled traffic within their respective WLANs

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
tunneled-vlan <VLAN-ID>
```

Parameters

```
tunneled-vlan <VLAN-ID>
```

tunneled-vlan <VLAN-ID>	Specifies the VLANs associated with this GRE tunnel • <VLAN-ID> – Specify the VLAN IDs. Specify a comma-separated list of IDs, to specify multiple VLANs. For example, 1,10,12,16-20

Example

```
rfs4000-229D58(config-device
00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#tunneled-vlan 10

rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#show
context
 gre tunnel testGRETunnel
  peer 1 ip 192.168.13.6
  native vlan 1
  tunneled-vlan 1,10
  native tagged
```

```
  dscp 20
  failover interval 200 retry 5
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#
```

Related Commands:

no	Removes the GRE tunnel settings based on the parameters passed

http-analyze

Profile Config Commands

Enables HTTP analysis on this profile. Use this command to configure the mode and interval at which data is sent to the controller (running the HTTP analytics engine).

In the Mobility 5.5 hierarchically organized network, HTTP analytics data forwarding is a simple and transparent process. The site controllers (Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000) receive the HTTP data from adopted APs adopted. This data is compressed and forwarded to the *Network Operations Center* (NOC) controller. The NOC controller caches, formats, and uploads this information to the external analytics engine. There is no need for a separate configuration to enable this feature.

For more information on the hierarchically network, see *device-upgrade*.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
http-analyze [compress|update-interval <1-3600>]
```

Parameters

```
http-analyze [compress|update-interval <1-3600>]
```

http-analyze	Configures HTTP analysis parameters. These parameters are: compress and update-interval.
compress	Compresses update files before forwarding to the controller. This option is disabled by default.
update-interval <1-3600>	Sets the interval, in seconds, at which buffered packets are pushed to analyze the HTTP connection • <1-3600> – Specify the interval from 1 - 3600 seconds. The default is 60 seconds.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#http-analyze compress
rfs7000-37FABE(config-profile-default-rfs7000)#

rfs7000-37FABE(config-profile-default-rfs7000)#http-analyze update-interval
200
rfs7000-37FABE(config-profile-default-rfs7000)#

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 bridge vlan 1
```

```
 ip igmp snooping
 ip igmp snooping querier
autoinstall configuration
autoinstall firmware
crypto ikev1 policy ikev1-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ikev2 policy ikev2-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
.................................................................
 qos trust 802.1p
interface pppoe1
use firewall-policy default
http-analyze update-interval 200
http-analyze compress
service pm sys-restart
router ospf
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Disables HTTP analyze settings

interface

Profile Config Commands

The following table summarizes interface configuration commands.

Command	Description	Reference
interface	Selects an interface to configure	page 653
interface-config-instance	Summarizes Ethernet interface (associated with the wireless controller or service platform) configuration commands	page 656
interface-config-vlan-instance	Summarizes VLAN interface configuration commands	page 675
interface-config-radio-instance	Summarizes radio interface configuration commands (applicable to devices with built-in radios)	page 684
interface-config-wwan-instance	Summarizes WWAN interface configuration commands	page 733

interface

interface

Selects an interface to configure

This command is used to enter the interface configuration mode for the specified physical SVI interface. If the VLAN (SVI) interface does not exist, it is automatically created.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax: Service Platforms

```
interface [<INTERFACE-NAME>|fe <1-4>|ge <1-24>|me1|port-channel <1-4>|pppoe1|
          radio [1|2|3]|serial <1-4>|t1e1 <1-4>|up <1-2>|vlan <1-4094>|vmif
<1-8>|wwan1|
          xge <1-4>]
```

Syntax: Access Points and Wireless Controllers

```
interface [<INTERFACE-NAME>|fe <1-4>|ge <1-8>|me1|port-channel <1-4>|pppoe1|
          radio [1|2|3]|up1|vlan <1-4094>|wwan1|xge <1-4>]
```

Parameters

```
interface [<INTERFACE-NAME>|fe <1-4>|fr <1-4>|ge <1-8>|me1|port-channel <1-4>|
radio [1|2|3]|serial <1-4>|t1e1 <1-4>|up1|vlan <1-4094>|vmif <1-8>|wwan1|xge
<1-4>]
```

<INTERFACE-NAME>	Enters the configuration mode of the interface identified by the <INTERFACE-NAME> keyword
fe <1-4>	Selects a FastEthernet interface • <1-4> – Specify the interface index from 1 - 4. This interface is applicable only for Brocade Mobility 6511 Access Point
ge <1-8>	Selects a GigabitEthernet interface • <1-8> – Specify the interface index from 1 - 8. (4 for Brocade Mobility RFS7000 and 8 for Brocade Mobility RFS6000).
me1	Selects a management interface Not applicable for Brocade Mobility RFS4000 The management interface is applicable only for Brocade Mobility RFS6000 and Brocade Mobility RFS7000
port-channel <1-4>	Selects the port channel interface • <1-4> – Specify the interface index from 1 - 4.
pppoe1	Selects the PPP over Ethernet interface to configure
radio [1|2|3]	Selects a radio interface • 1 – Selects radio interface 1 • 2 – Selects radio interface 2 • 3 – Selects radio interface 3 The radio interface is not available on wireless controllers (exception RFS4011) or service platforms.
serial <1-4>	Selects a serial interface • <1-4> – Specify the interface index from 1 - 4.
up1	Selects the uplink GigabitEthernet interface
vlan <1-4094>	Selects a VLAN interface • <1-4094> – Specify the SVI VLAN ID from 1 - 4094.
wwan1	Selects a Wireless WAN interface This interface is applicable only to Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point, AP82XX, Brocade Mobility RFS4000, Brocade Mobility RFS6000
xge <1-4>	Selects a TenGigabitEthernet interface • <1-2> – Specify the interface index from 1 - 4.

Usage Guidelines:

The ports available on a device vary depending on the model. The following ports are available on Brocade Mobility RFS4000, Brocade Mobility RFS6000 and Brocade Mobility RFS7000 model wireless controllers:

Brocade Mobility RFS4000 - ge1, ge2, ge3, ge4, ge5, up1

Brocade Mobility RFS6000 - ge1, ge2, ge3, ge4, ge5, ge6, ge7, ge8, me1, up1

Brocade Mobility RFS7000 - ge1, ge2, ge3, ge4, me1

The ports available on service platforms also vary depending on the model.

GE ports are available on Brocade Mobility RFS4000, Brocade Mobility RFS6000 and Brocade Mobility RFS7000 controllers. GE ports are RJ-45 supporting 10/100/1000Mbps. GE ports on the Brocade Mobility RFS7000 can be RJ-45 or fiber ports supporting 10/100/1000Mbps.

ME ports are available on Brocade Mobility RFS6000 and Brocade Mobility RFS7000 platforms. ME ports are out-of-band management ports used to manage the controller via CLI or Web UI, even when the other ports on the controller are unreachable.

UP ports are available on Brocade Mobility RFS4000 and Brocade Mobility RFS6000 platforms. A UP port is used to connect to the backbone network. UP ports are available on Brocade Mobility RFS4000 and Brocade Mobility RFS6000 controllers. A UP port supports either RJ-45 or fiber. The UP port is the preferred means to connect to the backbone as it has a non-blocking 1gbps connection unlike the GE ports.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan44)#
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan44)#?
SVI configuration commands:
  crypto               Encryption module
  description          Vlan description
  dhcp-relay-incoming  Allow on-board DHCP server to respond to relayed DHCP
                       packets on this interface
  ip                   Interface Internet Protocol config commands
  no                   Negate a command or set its defaults
  shutdown             Shutdown the selected interface
  use                  Set setting to use

  clrscr               Clears the display screen
  commit               Commit all changes made in this session
  do                   Run commands from Exec mode
  end                  End current mode and change to EXEC mode
  exit                 End current mode and down to previous mode
  help                 Description of the interactive help system
  revert               Revert changes
  service              Service Commands
  show                 Show running system information
  write                Write running configuration to memory or terminal

rfs7000-37FABE(config-profile-default-rfs7000-if-vlan44)#

nx4500-5CFA2B(config-profile-testNX45XX)#interface vmif 2
nx4500-5CFA2B(config-profile-testNX45XX-if-vmif12)#

nx4500-5CFA2B(config-profile-testNX45XX-if-vmif2)#?
VM Interface Mode commands:
  description  Port description
```

```
  ip           Internet Protocol (IP)
  no           Negate a command or set its defaults
  qos          Quality of service
  switchport   Set switching mode characteristics
  use          Set setting to use

  clrscr       Clears the display screen
  commit       Commit all changes made in this session
  do           Run commands from Exec mode
  end          End current mode and change to EXEC mode
  exit         End current mode and down to previous mode
  help         Description of the interactive help system
  revert       Revert changes
  service      Service Commands
  show         Show running system information
  write        Write running configuration to memory or terminal

nx4500-5CFA2B(config-profile-testNX45XX-if-vmif2)#
```

Related Commands:

no	Removes the selected interface

interface-config-instance

interface

Use the config-profile-<PROFILE-NAME> instance to configure the Ethernet, VLAN and tunnel associated with the
access point, wireless controller, or service platform.

To switch to this mode, use the following command:

```
<DEVICE>(config-profile-<DEVICE-PROFILE-NAME>)#interface [<INTERFACE-NAME>|fe
<1-4>|
ge <1-8>|me1|port-channel <1-4>|pppoe1|radio [1|2|3]|up1|vlan
<1-4094>|wwan1|xge <1-4>]
<DEVICE>(config-profile-default-rfs7000)# ge 1

The following example uses the config-profile-default-rfs7000 instance to
configure a GigabitEthernet interface:

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#?
Interface configuration commands:
  cdp            Cisco Discovery Protocol
  channel-group  Channel group commands
  description    Interface specific description
  dot1x          802.1X
  duplex         Set duplex to interface
  ip             Internet Protocol (IP)
  lldp           Link Local Discovery Protocol
  mac-auth       Enable mac-auth for this port
  no             Negate a command or set its defaults
  power          PoE Command
  qos            Quality of service
  shutdown       Shutdown the selected interface
  spanning-tree  Spanning tree commands
  speed          Configure speed
  switchport     Set switching mode characteristics
```

```
use             Set setting to use

clrscr          Clears the display screen
commit          Commit all changes made in this session
do              Run commands from Exec mode
end             End current mode and change to EXEC mode
exit            End current mode and down to previous mode
help            Description of the interactive help system
revert          Revert changes
service         Service Commands
show            Show running system information
write           Write running configuration to memory or terminal

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#
```

The following table summarizes the interface configuration commands.

Command	Description	Reference
cdp	Enables *Cisco Discovery Protocol* (CDP) on GE ports	page 658
channel-group	Configures channel group commands	*page 7-658*
description	Creates an interface specific description	*page 7-659*
dot1x (authenticator)	Configures 802.1X authenticator settings	page 660
dot1x (supplicant)	Configures 802.1X supplicant settings	page 661
duplex	Specifies the duplex mode for the interface	*page 7-662*
ip	Sets the IP address for the assigned Fast Ethernet interface (ME) and VLAN interface	*page 7-663*
lldp	Configures *Link Local Discovery Protocol* (LLDP)	*page 7-664*
mac-auth	Enables MAC-based port authentication on this profile	page 665
no	Negates a command or sets its defaults	*page 7-666*
power	Configures *Power over Ethernet* (PoE) settings on this interface	page 667
qos	Enables QoS	*page 7-668*
shutdown	Disables the selected interface	*page 7-668*
spanning-tree	Configures spanning tree parameters	*page 7-669*
speed	Specifies the speed of a FastEthernet or GigabitEthernet port	*page 7-671*
switchport	Sets interface switching mode characteristics	*page 7-672*
use	Defines the settings to use with this command	*page 7-674*
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	*page 5-394*
service	Invokes service commands to troubleshoot or debug (config-if) instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to the memory or terminal	page 425

cdp

interface-config-instance

Enables CDP on the selected GE port

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
cdp [receive|transmit]
```

Parameters

```
cdp [receive|transmit]
```

transmit	Enables CDP packet snooping on an interface
receive	Enables CDP packet transmission on an interface

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#cdp transmit
```

Related Commands:

no	Disables CDP on the controller or service platform's selected GE ports

channel-group

interface-config-instance

Configures a channel group

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
channel-group <1-4>
```

Parameters

```
channel-group <1-4>
```

<1-4>	Specifies a channel group number from 1 - 4

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#channel-group 1

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#show context
 interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
  channel-group 1
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#
```

Related Commands:

no	Removes a channel group

description

interface-config-instance

Configures a description for a defined interface

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
description [<LINE>|<WORD>]
```

Parameters

```
description [<LINE>|<WORD>]
```

<LINE>	Configures the maximum length (number of characters) of the interface description
<WORD>	Configures a unique description for this interface. The description should not exceed the length specified by the <LINE> parameter

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#description “This is
GigabitEthernet interface for Royal King”

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#show context
 interface ge1
  description This\ is\ GigabitEthernet\ interface\ for\ Royal\ King
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
  channel-group 1
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#
```

Related Commands:

no	Removes the interface description

dot1x (authenticator)

interface-config-instance

Configures 802.1X authenticator settings

Dot1x (or 802.1x) is an IEEE standard for network authentication. It enables media-level (layer 2) access control, providing the capability to permit or deny connectivity based on user or device identity. Dot1x allows port-based access using authentication. An dot1x enabled port can be dynamically enabled or disabled depending on user identity or device connection.

Devices supporting dot1x allow the automatic provision and connection to the wireless network without launching a Web browser at login. When within range of a dot1x network, a device automatically connects and authenticates without needing to manually login.

Before authentication, the endpoint is unknown, and traffic is blocked. Upon authentication, the endpoint is known and traffic is allowed. The controller or service platform uses source MAC filtering to ensure only the authenticated endpoint is allowed to send traffic.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
dot1x authenticator
[guest-vlan|host-mode|max-reauth-req|port-control|reauthenticate|
          timeout]

dot1x authenticator [guest-vlan <1-4094>|host-mode [multi-host|single-host]|
          max-reauth-req <1-10>|port-control
[auto|force-authorized|force-unauthorized]|
          reauthenticate|timeout [quiet-period|reauth-period] <1-65535>]
```

NOTE
The dot1x (802.1x) supplicant settings are documented in the next section.

Parameters

```
dot1x authenticator [guest-vlan <1-4094>|host-mode [multi-host|single-host]|
max-reauth-req <1-10>|port-control
[auto|force-authorized|force-unauthorized]|
reauthenticate|timeout [quiet-period|reauth-period]]
```

dot1x authenticator	Configures 802.1x authenticator settings
guest-vlan <1-4094>	Configures the guest VLAN for this interface. This is the VLAN traffic is bridged on if this port is unauthorized and the guest VLAN is globally enabled. Select the VLAN index from 1 - 4094.

host-mode [multi-host|single-host]	Configures the host mode for this interface • multi-host – Configures multiple host mode • single-host – Configures single host mode. This is the default setting.
max-reauth-req <1-10>	Configures maximum number of reauthorization retries for the supplicant. This is the maximum number of reauthentication attempts made before this port is moved to unauthorized. • <1-10> – Specify a value from 1 -10. The default is 2.
port-control [auto|force-authorized|force-unauthorized]	Configures port control state • auto – Configures auto port state • force-authorized – Configures authorized port state. This is the default setting. • force-unauthorized – Configures unauthorized port state
reauthenticate	Enables or disables re-authentication for this port. When enabled, clients are forced to reauthenticate on this port. The setting is disabled by default. Therefore, clients are not required to reauthenticate for connection over this port until this setting is enabled.
timeout [quiet-period|reauth-period] <1-65535>	Configures timeout settings for this interface • quiet-period – Configures the quiet period timeout in seconds. This is the interval, in seconds, between successive client authentication attempts. • reauth-period – Configures the time after which re-authentication is initiated The following option is common to 'quiet-period' and 'reauth-period' keywords: • <1-65535> – Specify a 'quiet-period' or 'reauth-period' from 1 -65535 seconds.

Example

```
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-ge1)#dot1x
authenticator guest-vlan 2

rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-ge1)#dot1x
authenticator host-mode multi-host

rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-ge1)#dot1x
authenticator max-reauth-req 6

rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-ge1)#dot1x
authenticator reauthenticate

rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-ge1)#show
context
 interface ge1
  dot1x authenticator host-mode multi-host
  dot1x authenticator guest-vlan 2
  dot1x authenticator reauthenticate
  dot1x authenticator max-reauth-count 6
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-ge1)#
```

Related Commands:

no	Disables or reverts interface settings to their default

dot1x (supplicant)

interface-config-instance

Configures 802.1X supplicant (client) settings

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
dot1x supplicant username <USERNAME> password [0 <WORD>|2 <WORD>|<WORD>]
```

Parameters

```
dot1x supplicant username <USERNAME> password [0 <WORD>|2 <WORD>|<WORD>]
```

dot1x supplicant	Configures 802.1x suppliant settings
username <USERNAME>	Sets the username for authentication • <USERNAME> – Specify the supplicant's username.
password [0 <WORD>| 2 <WORD>|<WORD>]	Sets the password associated with the supplicant's username. Select any one of the following options: • 0 <WORD> – Sets a clear text password • 2 <WORD> – Sets an encrypted password • <WORD> – Specify the password.

Example

```
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-ge1)#dot1x
supplicant username bob
password 0 motorolasolutions@123

rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-ge1)#show
context
 interface ge1
  dot1x supplicant username bob password 0 motorolasolutions@123
  dot1x authenticator host-mode multi-host
  dot1x authenticator guest-vlan 2
  dot1x authenticator reauthenticate
  dot1x authenticator max-reauth-count 6
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-ge1)#
```

Related Commands:

no	Removes 802.1X supplicant (client) settings

duplex

interface-config-instance

Configures duplex mode (for the flow of packets) for an interface

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
duplex [auto|half|full]
```

Parameters

```
duplex [auto|half|full]
```

auto	Enables automatic duplexity on an interface port. The port automatically detects whether it should run in full or half-duplex mode. (default setting)
half	Sets the port to half-duplex mode. Allows communication in one direction only at any given time
full	Sets the port to full-duplex mode. Allows communication in both directions simultaneously

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#duplex full

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#show context
 interface ge1
  description This\ is\ GigabitEthernet\ interface\ for\ Royal\ King
  duplex full
  dot1x supplicant username Bob password 0 motorolasolutions@123
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
  channel-group 1
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#
```

Related Commands:

no	Reverts to default (auto)

ip

interface-config-instance

Sets the ARP and DHCP components for this interface

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
ip [arp|dhcp]

ip [arp [header-mismatch-validation|trust]|dhcp trust]
```

Parameters

```
ip [arp [header-mismatch-validation|trust]|dhcp trust]
```

arp [header-mismatch-validation|trust]	Sets ARP for packets on this interface • header-mismatch-validation – Verifies mismatch for source MAC address in the ARP header and Ethernet header • trust – Sets the ARP trust state for ARP responses on this interface
dhcp trust	Uses a DHCP client to obtain an IP address for the interface (this enables DHCP on a layer 3 SVI) • trust – Sets the DHCP trust state for DHXP responses on this interface

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#ip dhcp trust

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#ip arp
header-mismatch-validation

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#show context
 interface ge1
  description This\ is\ GigabitEthernet\ interface\ for\ Royal\ King
  duplex full
  dot1x supplicant username Bob password 0 motorolasolutions@123
  ip dhcp trust
  ip arp header-mismatch-validation
  qos trust dscp
  qos trust 802.1p
  channel-group 1
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#
```

Related Commands:

no	Removes the ARP and DHCP components configured for this interface

lldp

interface-config-instance

Configures *Link Local Discovery Protocol* (LLDP) parameters on the selected interface

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
lldp [receive|transmit]
```

Parameters

```
lldp [receive|transmit]
```

[receive]	Enables LLDP *Protocol Data Units* (PDUs) snooping
transmit	Enables LLDP PDUs transmission

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#lldp transmit
```

Related Commands:

no	Disables or reverts interface settings to their default

mac-auth

interface-config-instance

Enables authentication of MAC addresses on the selected wired port. Devices using this profile will be able be to authenticate the MAC addresses of devices connecting to this GE interface

When enabled, this feature authenticates the source MAC address of a device, connecting to this interface, with a RADIUS server. For more information on enabling this feature see, *mac-auth*.

To enable MAC address authentication on a device, execute the *mac-auth* command on the device configuration mode.

Supported in the following platforms:

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
mac-auth
```

Parameters

None

Example

```
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-ge1)#mac-auth
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-ge1)#

rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-ge1)#show
context
 interface ge1
  mac-auth
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
  channel-group 1
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-ge1)#

rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-ge5)#mac-auth
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-ge5)#

rfs4000-229D58(config-device-00-23-68-22-9D-58-if-ge5)#show context
 interface ge5
  switchport mode access
  switchport access vlan 1
  dot1x authenticator host-mode single-host
  dot1x authenticator guest-vlan 5
  dot1x authenticator port-control auto
  mac-auth
rfs4000-229D58(config-device-00-23-68-22-9D-58-if-ge5)#
```

Related Commands:

no	Disables authentication of MAC addresses on the selected wired port

no

interface-config-instance

Negates a command or sets its defaults

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no
[cdp|channel-group|description|dot1x|duplex|ip|lldp|mac-auth|power|qos|shutdo
wn|
          spanning-tree|speed|switchport|use]
```

Parameters

None

Usage Guidelines:

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#no cdp

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#no duplex
```

Related Commands:

cdp	Enables CDP on ports
channel-group	Configures channel group commands
description	Creates an interface specific description
dot1x (authenticator)	Configures 802.1X authentication settings
duplex	Specifies the duplex mode for the interface
ip	Sets the IP address for the assigned Fast Ethernet interface (ME) and VLAN interface
lldp	Configures LLDP
mac-auth	Enables MAC-based port authentication on this profile
power	Configures PoE settings on this interface
qos	Enables QoS on the selected interface

shutdown	Disables the selected interface
spanning-tree	Configures spanning tree parameters
speed	Specifies the speed of a FastEthernet or GigabitEthernet port
switchport	Sets the interface switching mode characteristics
use	Defines the settings to use with this command
write	Writes information to the memory or terminal

power

interface-config-instance

Configures PoE settings on this interface

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
power {limit <0-40>|priority [critical|high|low]}
```

Parameters

```
power {limit <0-40>|priority [critical|high|low]}
```

power	Configures power related thresholds for this interface
limit <0-40>	Optional. Configures the PoE power limit from 0 - 40 Watts
priority [critical|high|low]	Optional. Configures the PoE power priority on this interface • critical – Sets PoE priority as critical • high – Sets PoE priority as high • low – Sets PoE priority as low

Example

```
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-ge1)#power
limit 30

rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-ge1)#power
priority critical

rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-ge1)#show
context
 interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
  power limit 30
  power priority critical
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-ge1)#
```

Related Commands:

no	Removes PoE settings on this interface

qos

interface-config-instance

Defines *Quality of Service* (QoS) settings on this interface

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
qos trust [802.1p|cos|dscp]
```

Parameters

```
qos trust [802.1p|cos|dscp]
```

trust [802.1p|cos|dscp]	Trusts QoS values ingressing on this interface • 802.1p – Trusts 802.1p COS values ingressing on this interface • cos – Trusts 802.1p COS values ingressing on this interface • dscp – Trusts IP DSCP QOS values ingressing on this interface

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#qos trust dscp

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#qos trust 802.1p

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#show context
 interface ge1
  description This\ is\ GigabitEthernet\ interface\ for\ Royal\ King
  duplex full
  dot1x supplicant username Bob password 0 motorolasolutions@123
  ip dhcp trust
  ip arp header-mismatch-validation
  qos trust dscp
  qos trust 802.1p
  channel-group 1
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#
```

Related Commands:

no	Removes QoS settings on the selected interface

shutdown

interface-config-instance

Shuts down (disables) an interface. The interface is administratively enabled unless explicitly disabled using this command.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
shutdown
```

Parameters

None

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#shutdown
```

Related Commands:

no	Disables or reverts interface settings to their default

spanning-tree

interface-config-instance

Configures spanning tree parameters

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
spanning-tree
[bpdufilter|bpduguard|edgeport|force-version|guard|link-type|mst|
          port-cisco-interoperability|portfast]

spanning-tree [edgeport|force-version <0-3>|guard root|portfast]

spanning-tree [bpdufilter|bpduguard] [default|disable|enable]

spanning-tree link-type [point-to-point|shared]

spanning-tree mst <0-15> [cost <1-200000000>|port-priority <0-240>]

spanning-tree port-cisco-interoperability [disable|enable]
```

Parameters

`spanning-tree [edgeport|force-version|guard root|portfast]`

edgeport	Enables an interface as an edge port
force-version <0-3>	Specifies the spanning tree force version. A version identifier of less than 2 enforces the spanning tree protocol. Select one of the following versions: • 0 – *Spanning Tree Protocol* (STP) • 1 – Not supported • 2 – *Rapid Spanning tree Protocol* (RSTP) • 3 – *Multiple Spanning Tree Protocol* (MSTP) (default setting)
guard root	Enables Root Guard for the port The Root Guard disables superior *Bridge Protocol Data Unit* (BPDU) reception. The Root Guard ensures the enabled port is a designated port. If the Root Guard enabled port receives a superior BPDU, it moves to a discarding state. Use the no parameter with this command to disable the Root Guard.
portfast	Enables rapid transitions. Enabling PortFast allows the port to bypass the listening and learning states

`spanning-tree [bpdufilter|bpduguard] [default|disable|enable]`

bpdufilter [default|disable|enable]	Sets a PortFast BPDU filter for the port Use the no parameter with this command to revert the port BPDU filter to its default. The spanning tree protocol sends BPDUs from all ports. Enabling the BPDU filter ensures PortFast enabled ports do not transmit or receive BPDUs.
bpduguard [default|disable|enable]	Enables or disables BPDU guard on a port Use the no parameter with this command to set BPDU guard to its default. When the BPDU guard is set for a bridge, all PortFast-enabled ports that have the BPDU guard set to default shut down upon receiving a BPDU. If this occurs, the BPDU is not processed. The port can be brought back either manually (using the no shutdown command), or by configuring the errdisable-timeout to enable the port after a specified interval.

`spanning-tree link-type [point-to-point|shared]`

link-type [point-to-point|shared]	Enables or disables point-to-point or shared link types • point-to-point – Enables rapid transition • shared – Disables rapid transition

`spanning-tree mst <0-15> [cost <1-200000000>|port-priority <0-240>]`

mst <0-15>	Configures MST on a spanning tree
cost <1-200000000>	Defines path cost for a port from 1 - 200000000
port-priority <0-240>	Defines port priority for a bridge from 1 - 240

`spanning-tree port-cisco-interoperability [disable[a]|enable]]`

port-cisco-interoperability	Enables or disables interoperability with Cisco's version of MSTP (which is incompatible with standard MSTP)
enable	Enables CISCO Interoperability
disable	Disables CISCO Interoperability. The default is disabled.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#spanning-tree
bpdufilter disable

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#spanning-tree bpduguard
enable
```

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#spanning-tree
force-version 1

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#spanning-tree guard
root

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#spanning-tree mst 2
port-priority 10

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#show context
 interface ge1
  description This\ is\ GigabitEthernet\ interface\ for\ Royal\ King
  duplex full
  spanning-tree bpduguard enable
  spanning-tree bpdufilter disable
  spanning-tree force-version 1
  spanning-tree guard root
  spanning-tree mst 2 port-priority 10
 --More--
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#
```

Related Commands:

no	Removes spanning tree settings configured on this interface

speed

interface-config-instance

Specifies the speed of a FastEthernet (10/100) or GigabitEthernet (10/100/1000) port

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
speed [10|100|1000|auto]
```

Parameters

```
speed [10|100|1000|auto]
```

10	Forces 10 Mbps operation
100	Forces 100 Mbps operation
1000	Forces 1000 Mbps operation
auto	Port automatically detects its operational speed based on the port at the other end of the link. Auto negotiation is a requirement for using 1000BASE-T[3] according to the standard (default setting).

Usage Guidelines:

Set the interface speed to auto detect and use the fastest speed available. Speed detection is based on connected network hardware.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#speed 10

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#show context
 interface ge1
  description This\ is\ GigabitEthernet\ interface\ for\ Royal\ King
  speed 10
  duplex full
  spanning-tree bpduguard enable
  spanning-tree bpdufilter disable
  spanning-tree force-version 1
  spanning-tree guard root
  spanning-tree mst 2 port-priority 10
  dot1x supplicant username Bob password 0 motorolasolutions@123
  ip dhcp trust
  ip arp header-mismatch-validation
  qos trust dscp
  qos trust 802.1p
  channel-group 1
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#
```

Related Commands:

no	Resets speed to default (auto)

switchport

interface-config-instance

Sets switching mode characteristics for the selected interface

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
switchport [access|mode|trunk]

switchport access vlan <1-4094>
switchport mode [access|trunk]
switchport trunk [allowed|native]
switchport trunk allowed vlan [<VLAN-ID>|add <VLAN-ID>|none|remove <VLAN-ID>]
switchport trunk native [tagged|vlan <1-4094>]
```

Parameters

```
switchport access vlan <1-4094>
```

access vlan <1-4094>	Sets the VLAN when interface is in the access mode • <1-4094> – Specify the SVI VLAN ID from 1 - 4094.

`switchport mode [access|trunk]`

mode [access|trunk]	Sets the interface mode to access or trunk (can only be used on physical - layer 2 - interfaces) • access – If access mode is selected, the access VLAN is automatically set to VLAN1. In this mode, only untagged packets in the access VLAN (vlan1) are accepted on this port. All tagged packets are discarded. • trunk – If trunk mode is selected, tagged VLAN packets are accepted. The native VLAN is automatically set to VLAN1. Untagged packets are placed in the native VLAN by the wireless controller or service platform. Outgoing packets in the native VLAN are sent untagged. The default mode for both ports is trunk.

`switchport trunk allowed vlan [<VLAN-ID>|add <VLAN-ID>|none|remove <VLAN-ID>]`

trunk	Sets trunking mode characteristics of the port
allowed	Configures trunk characteristics when the port is in trunk mode
vlan [<VLAN-ID>| add <VLAN-ID>| none| remove <VLAN-ID>	Sets allowed VLAN options. The options are: • <VLAN-ID> – Allows a group of VLAN IDs. Specify the VLAN IDs, can be either a range (55-60) or a comma-separated list (35, 41 etc.) • none – Allows no VLANs to transmit or receive through the layer 2 interface • add <VLAN-ID> – Adds VLANs to the current list • <VLAN-ID> – Specify the VLAN IDs. Can be either a range of VLAN (55-60) or a list of comma separated IDs (35, 41 etc.) • remove <VLAN-ID> – Removes VLANs from the current list • <VLAN-ID> – Specify the VLAN IDs. Can be either a range of VLAN (55-60) or a list of comma separated IDs (35, 41 etc.)

`switchport trunk native [tagged|vlan <1-4094>]`

trunk	Sets trunking mode characteristics of the switchport
native [tagged|vlan <1-4094>]	Configures the native VLAN ID for the trunk-mode port • tagged – Tags the native VLAN • vlan <1-4094> – Sets the native VLAN for classifying untagged traffic when the interface is in trunking mode. Specify a value from 1 - 4094.

Usage Guidelines:

Interfaces ge1 - ge4 can be configured as trunk or in access mode. An interface configured as “trunk” allows packets (from the given list of VLANs) to be added to the trunk. An interface configured as “access” allows packets only from native VLANs.

Use the [no] switchport (access|mode|trunk)to undo switchport configurations

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#switchport trunk native
tagged

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#switchport access vlan
1

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#show context
 interface ge1
  description This\ is\ GigabitEthernet\ interface\ for\ Royal\ King
  speed 10
  duplex full
  switchport mode access
  switchport access vlan 1
  spanning-tree bpduguard enable
  spanning-tree bpdufilter disable
```

```
  spanning-tree force-version 1
  spanning-tree guard root
  spanning-tree mst 2 port-priority 10
  dot1x supplicant username Bob password 0 motorolasolutions@123
  ip dhcp trust
  ip arp header-mismatch-validation
  qos trust dscp
  qos trust 802.1p
  channel-group 1
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#
```

Related Commands:

no	Disables or reverts interface settings to their default

use

interface-config-instance

Specifies the IP access list and MAC access list used with this interface

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
use [ip-access-list in <IP-ACCESS-LIST-NAME>|mac-access-list in
<MAC-ACCESS-LIST-NAME>]
```

Parameters

```
use [ip-access-list in <IP-ACCESS-LIST-NAME>|mac-access-list in
<MAC-ACCESS-LIST-NAME>]
```

ip-access-list in <IP-ACCESS-LIST-NAME>	Uses an IP access list • in – Applies an ACL on incoming packets • <IP-ACCESS-LIST-NAME> – Specify the IP access list name (it should be an existing and configured).
mac-access-list in <MAC-ACCESS-LIST-NAME>	Uses a MAC access list • in – Applies an ACL on incoming packets • <MAC-ACCESS-LIST-NAME> – Specify the MAC access list name (it should be an existing and configured).

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#use mac-access-list in
test

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#show context
 interface ge1
  description This\ is\ GigabitEthernet\ interface\ for\ Royal\ King
  speed 10
  duplex full
```

```
  switchport mode access
  switchport access vlan 1
  use ip-access-list in test
  use mac-access-list in test
  spanning-tree bpduguard enable
  spanning-tree bpdufilter disable
  spanning-tree force-version 1
  spanning-tree guard root
  spanning-tree mst 2 port-priority 10
  dot1x supplicant username Bob password 0 motorolasolutions@123
  ip dhcp trust
  ip arp header-mismatch-validation
  qos trust dscp
  qos trust 802.1p
  channel-group 1
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#
```

Related Commands:

no	Disassociates the IP access list or MAC access list from the interface

interface-config-vlan-instance

interface

Use the config-profile-<DEVICE-PROFILE-NAME> mode to configure Ethernet, VLAN and tunnel settings.

To switch to this mode, use the following commands:

```
<DEVICE>(config-profile-default-rfs7000<DEVICE-RPFILEPROFILE-NAME>)#interface
[<INTERFACE-NAME>|fe <1-4>|ge <1-8>|me1|port-channel <1-4>|pppoe1|radio
[1|2|3]|up1|vlan <1-4094>|wwan1|xge <1-24>]
```

The following example uses the config-profile-default-rfs7000 instance to configure a VLAN interface:

```
rfs7000-37FABE(config-profile-default-rfs7000)#interface vlan 8
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#

rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#?
SVI configuration commands:
  crypto               Encryption module
  description          Vlan description
  dhcp-relay-incoming  Allow on-board DHCP server to respond to relayed DHCP
                       packets on this interface
  ip                   Interface Internet Protocol config commands
  no                   Negate a command or set its defaults
  shutdown             Shutdown the selected interface
  use                  Set setting to use

  clrscr               Clears the display screen
  commit               Commit all changes made in this session
  do                   Run commands from Exec mode
  end                  End current mode and change to EXEC mode
  exit                 End current mode and down to previous mode
  help                 Description of the interactive help system
  revert               Revert changes
  service              Service Commands
  show                 Show running system information
```

```
  write                Write running configuration to memory or terminal

rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#
```

The following table summarizes interface VLAN configuration commands.

Commands	Description	Reference
crypto	Defines the encryption module	page 676
description	Defines the VLAN interface description	*page 7-677*
dhcp-relay-incoming	Allows an onboard DHCP server to respond to relayed DHCP packets on this interface	page 678
ip	Configures *Internet Protocol* (IP) config commands	page 678
no	Negates a command or sets its default	*page 7-680*
shutdown	Shuts down an interface	*page 7-683*
use	Defines the settings used with this command	*page 7-684*
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug (config-if) instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

crypto

interface-config-vlan-instance

Sets encryption module for this VLAN interface. The encryption module (crypto map) is configured using the crypto map command. For more information, see *crypto*.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
crypto map <CRYPTO-MAP-NAME>
```

Parameters

```
crypto map <CRYPTO-MAP-NAME>
```

map <CRYPTO-MAP-NAME>	Attaches a crypto map to the selected VLAN interface. The crypto map should be existing and configured. • <CRYPTO-MAP-NAME> – Specify the crypto map name.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#crypto map map1

rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#show context
 interface vlan8
  crypto map map1
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#
```

Related Commands:

no	Disables or reverts interface VLAN settings to their default

description

interface-config-vlan-instance

Defines a VLAN interface description. Use this command to provide additional information about the VLAN.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
description <WORD>
```

Parameters

```
description <WORD>
```

description <WORD>	Configures a description for this VLAN interface

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#description “This
VLAN interface is configured for the Sales Team”

rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#show context
 interface vlan8
  description This\ VLAN\ interface\ is\ configured\ for\ the\ Sales\ Team
  crypto map map1
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#
```

Related Commands:

no	Removes the VLAN interface description

dhcp-relay-incoming

interface-config-vlan-instance

Allows an onboard DHCP server to respond to relayed DHCP packets

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
dhcp-relay-incoming
```

Parameters

None

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#dhcp-relay-incoming

rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#show context
 interface vlan8
  description This\ VLAN\ interface\ is\ configured\ for\ the\ Sales\ Team
  crypto map map1
  dhcp-relay-incoming
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#
```

Related Commands:

no	Disables or reverts interface VLAN settings to their default

ip

interface-config-vlan-instance

Configures the VLAN interface's IP settings

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
ip [address|dhcp|helper-address|nat|ospf]

ip helper-address <IP>
```

```
ip address [<IP/M>|dhcp|zerconf]
ip address [<IP/M> {secondary}|zeroconf {secondary}]

ip dhcp client request options all

ip nat [inside|outside]

ip ospf
[authentication|authentication-key|bandwidth|cost|message-digest-key|priority
]

ip ospf authentication [message-digest|null|simple-password]
ip ospf authentication-key simple-password [0 <WORD>|2 <WORD>]
ip ospf [bandwidth <1-10000000>|cost <1-65535>|priority <0-255>]
ip ospf message-digest-key key-id <1-255> md5 [0 <WORD>|2 <WORD>]
```

Parameters

`ip helper-address <IP>`

helper-address <IP>	Enables DHCP and BOOTP forwarding for a set of clients. Configure a helper address on the VLAN interface connected to the client. The helper address should specify the address of the BOOTP or DHCP servers. If you have multiple servers, configure one helper address for each server. • <IP> – Specify the IP address of the DHCP or BOOTP server.

`ip address [<IP/M> {secondary}|dhcp|zerconf {secondary}]`

address	Sets the VLAN interface IP address
<IP/M> {secondary}	Specifies the interface IP address in the A.B.C.D/M format • secondary – Optional. Sets the specified IP address as a secondary address
dhcp	Uses a DHCP client to obtain an IP address for this interface
zerconf {secondary}	Uses *Zero Configuration Networking* (zerconf) to generate an IP address for this interface • secondary – Optional. Sets the generated IP address as a secondary address

`ip dhcp client request options all`

dhcp	Uses a DHCP client to configure a request on this VLAN interface
client	Configures a DHCP client
request	Configures DHCP client request
options	Configures DHCP client request options
all	Configures all DHCP client request options

`ip nat [inside|outside]`

nat [inside|outside]	Defines NAT settings for the VLAN interface • inside – Sets the NAT inside interface • outside – Sets the NAT outside interface

`ip ospf authentication [message-digest|null|simple-password]`

ospf authentication	Configures OSPF authentication scheme. Options are message-digest, null, and simple-password.
message-digest	Configures md5 based authentication
null	No authentication required
simple-password	Configures simple password based authentication

`ip ospf authentication-key simple-password [0 <WORD>|2 <WORD>]`

ospf authentication-key	Configures an authentication key
simple-password [0 <WORD>|2 <WORD>]	Configures an authentication key for simple password authentication • 0 <WORD> – Configures clear text key • 2 <WORD> – Configures encrypted key

`ip ospf [bandwidth <1-10000000>|cost <1-65535>|priority <0-255>]`

bandwidth <1-10000000>	Configures bandwidth for the physical port mapped to this layer 3 interface • <1-10000000> – Specify the bandwidth from 1 -10000000.
cost <1-65535>	Configures OSPF cost • <1-65535> – Specify OSPF cost value from 1 - 65535.
priority <0-255>	Configures OSPF priority • <0-255> – Specify OSPF priority value from 0 - 255.

`ip ospf message-digest-key key-id <1-255> md5 [0 <WORD>|2 <WORD>]`

ospf message-digest	Configures message digest authentication parameters
key-id <1-255>	Configures message digest authentication key ID from 0 -255.
md5 [0 <WORD>|2 <WORD>]	Configures md5 key • 0 <WORD> – Configures clear text key • 2 <WORD> – Configures encrypted key

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#ip address 10.0.0.1/8

rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#ip nat inside

rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#ip helper-address
172.16.10.3

rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#ip dhcp client
request
options all

rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#show context
 interface vlan8
  description This\ VLAN\ interface\ is\ configured\ for\ the\ Sales\ Team
  ip address 10.0.0.1/8
  ip dhcp client request options all
  ip helper-address 172.16.10.3
  ip nat inside
  crypto map map1
  dhcp-relay-incoming
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#
```

Related Commands:

no	Removes or resets IP settings on this interface

no

interface-config-vlan-instance

Negates a command or reverts to defaults. The no command, when used in the Config Interface VLAN mode, negates VLAN interface settings or reverts them to their default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no [crypto|description|dhcp-relay-incoming|ip|shutdown|use]

no [crypto map|description|dhcp-relay-incoming|shutdown|use
<IP-ACCESS-LIST-NAME> in]

no ip [address|dhcp|helper-address|nat|ospf]
no ip [helper-address <IP>|nat]
no ip address [<IP/M> {secondary}|dhcp|zerconf {secondary}]
no ip dhcp client request options all
no ip ospf
[authentication|authentication-key|bandwidth|cost|message-digest-key|
          priority]
```

Parameters

```
no [crypto map|description|dhcp-relay-incoming|shutdown|use
<IP-ACCESS-LIST-NAME> in]
```

no crypto map	Disassociates a crypto map from an interface
no description	Removes the VLAN interface description
no dhcp-relay-incoming	Prevents an onboard DHCP server from responding to relayed DHCP packets
no shutdown	Enables an interface If an interface has been shutdown, use the no shutdown command to enable the interface. Use this command to trouble shoot new interfaces.
no use <IP-ACCESS-LIST-NAME> in	Removes specified IP access list from use by an interface • in – Disables incoming packets • <IP-ACCESS-LIST-NAME> – Specify the IP access list name.

```
no ip address [<IP/M> {secondary}|dhcp|zerconf {secondary}]
```

no ip address	Removes or reverts interface IP settings • address – Removes IP addresses configured for this interface
<IP/M> {secondary}	Specify the interface IP address in the A.B.C.D/M format. • secondary – Optional. Removes the secondary IP address
dhcp	Removes the IP address obtained using the DHCP client
zerconf {secondary}	Removes the IP address generated using a zerconf • secondary – Optional. Removes the secondary IP address

	`no ip address [helper-address <IP>|nat]`
no ip address	Removes or reverts interface IP settings • address – Removes IP addresses configured for this interface, depending on the options used while setting the address
helper-address <IP>	Disables the forwarding of DHCP and BOOTP packets to the configured helper IP address • <IP> – Specify the IP address of the DHCP or BOOTP server.
nat	Disables NAT for this interface

	`no ip address dhcp client request options all`
no ip address	Removes or reverts interface IP settings • address – Removes IP addresses configured for this interface, depending on the options used while setting the address
dhcp	Removes DHCP client request configured for this interface
client	Removes a DHCP client
request	Removes DHCP client request
options	Removes DHCP client request options
all	Removes all DHCP client request options

	`no ip ospf [authentication|authentication-key|bandwidth|cost|message-digest-key| priority]`
no ip ospf	Removes or reverts interface IP settings • ospf – Removes OSPF settings
authentication	Removes OSPF authentication scheme
authentication-key	Removes the authentication key associated with this layer 3 interface
bandwidth	Removes the bandwidth configured for the physical port mapped to this layer 3 interface
cost	Removes the OSPF cost configured for this layer 3 interface
message-digest-key <KEY-ID>	Removes the message digest authentication key identified by the <KEY-ID> keyword.
priority	Removes the OSPF priority configured for this layer 3 interface

Example

```
The following example shows the VLAN interface settings before the ‘no’
commands are executed:

rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#show context
 interface vlan8
  description This\ VLAN\ interface\ is\ configured\ for\ the\ Sales\ Team
  ip address 10.0.0.1/8
  ip dhcp client request options all
  ip helper-address 172.16.10.3
  ip nat inside
  crypto map map1
  dhcp-relay-incoming
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#

rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#no crypto map
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#no description
```

```
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#no
dhcp-relay-incoming
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#no ip dhcp client
request options all

The following example shows the VLAN interface settings after the 'no'
commands are executed:

rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#show context
 interface vlan8
  ip address 10.0.0.1/8
  ip helper-address 172.16.10.3
  ip nat inside
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#
```

Related Commands:

crypto	Defines the encryption module
description	Defines the VLAN description
dhcp-relay-incoming	Allows an onboard DHCP server to respond to relayed DHCP packets on this interface
ip	Configures IP config commands
shutdown	Disables an interface
use	Defines the settings used with this command

shutdown

interface-config-vlan-instance

Shuts down the selected interface. Use the no shutdown command to enable an interface.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
shutdown
```

Parameters

None

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#shutdown

rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#show context
 interface vlan8
  ip address 10.0.0.1/8
  ip helper-address 172.16.10.3
  shutdown
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#
```

Related Commands:

no	Disables or reverts interface VLAN settings to their default

use

interface-config-vlan-instance

Specifies an IP access list to use with this VLAN interface

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
use ip-access-list in <IP-ACCESS-LIST-NAME>
```

Parameters

```
use ip-access-list in <IP-ACCESS-LIST-NAME>
```

ip-access-list in <IP-ACCESS-LIST-NAME>	Uses a specified IP access list with this interface • in – Sets incoming packets • <IP-ACCESS-LIST-NAME> – Specify the IP access list name.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#use ip-access-list in
test

rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#show context
 interface vlan8
  ip address 10.0.0.1/8
  use ip-access-list in test
  ip helper-address 172.16.10.3
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#
```

Related Commands:

no	Disables or reverts interface VLAN settings to their default

interface-config-radio-instance

interface

This section documents radio interface configuration parameters applicable only to the access point profiles and the RFS4011 profile.

The access point radio interface can be radio1, radio2 or radio3. Legacy Brocade Mobility 71XX Access Point models contain either a single or a dual radio configuration. Newer Brocade Mobility 71XX Access PointN model access points support single, dual or triple radio configurations. An Brocade Mobility 650 Access Point model access point is available in either single or dual radio models. The remainder of the access point portfolio are dual-radio models.

To enter the AP profile > radio interface context, use the following commands:

```
<DEVICE>(config)#profile <AP-TYPE> <PROFILE-NAME>

rfs7000-37FABE(config)#profile br71xx 71xxTestProfile
rfs7000-37FABE(config-profile-71xxTestProfile)#

rfs7000-37FABE(config-profile-71xxTestProfile)#interface radio 1
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#?
Radio Mode commands:
  aeroscout                   Aeroscout Multicast MAC/Enable
  aggregation                 Configure 802.11n aggregation related parameters
  airtime-fairness            Enable fair access to medium for clients based on
                               their usage of airtime
  antenna-diversity           Transmit antenna diversity for non-11n transmit
                               rates
  antenna-downtilt            Enable ADEPT antenna mode
  antenna-gain                Specifies the antenna gain of this radio
  antenna-mode               Configure the antenna mode (number of transmit and
                               receive antennas) on the radio
  beacon                      Configure beacon parameters
  channel                    Configure the channel of operation for this radio
  data-rates                  Specify the 802.11 rates to be supported on this
                               radio
  description                 Configure a description for this radio
  dfs-rehome                  Revert to configured home channel once dfs
                               evacuation period expires
  dynamic-chain-selection     Automatic antenna-mode selection (single antenna
                               for non-11n transmit rates)
  ekahau                      Ekahau Multicast MAC/Enable
  extended-range              Configure extended range
  guard-interval              Configure the 802.11n guard interval
  ldpc                        Configure support for Low Density Parity Check
Code
  lock-rf-mode                Retain user configured rf-mode setting for this
                               radio
  max-clients                 Maximum number of wireless clients allowed to
                               associate subject to AP limit
  mesh                        Configure radio mesh parameters
  meshpoint                   Enable meshpoints on this radio
  no                          Negate a command or set its defaults
  non-unicast                 Configure handling of non-unicast frames
  off-channel-scan            Enable off-channel scanning on the radio
  placement                   Configure the location where this radio is
                               operating
  power                       Configure the transmit power of the radio
  preamble-short              Use short preambles on this radio
  probe-response              Configure transmission parameters for Probe
                               Response frames
  radio-resource-measurement  Configure support for 802.11k Radio Resource
                               Measurement
```

```
  radio-share-mode            Configure the radio-share mode of operation for
                              this radio
  rate-selection              Default or Opportunistic rate selection
  remove-override             Negate a command or set its defaults
  rf-mode                    Configure the rf-mode of operation for this radio
  rifs                       Configure Reduced Interframe Spacing (RIFS)
                             parameters
  rts-threshold              Configure the RTS threshold
  shutdown                   Shutdown the selected radio interface
  sniffer-redirect           Capture packets and redirect to an IP address
                             running a packet capture/analysis tool
  stbc                      Configure Space-Time Block Coding (STBC) parameters
  use                        Set setting to use
  wireless-client            Configure wireless client related parameters
  wlan                       Enable wlans on this radio

  clrscr                     Clears the display screen
  commit                     Commit all changes made in this session
  do                         Run commands from Exec mode
  end                        End current mode and change to EXEC mode
  exit                       End current mode and down to previous mode
  help                       Description of the interactive help system
  revert                     Revert changes
  service                    Service Commands
  show                       Show running system information
  write                     Write running configuration to memory or terminal

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

The following table summarizes the radio interface configuration commands.

Commands	Description	Reference
aeroscout	Enables Aeroscout multicast packet forwarding	*page 7-687*
aggregation	Configures 802.11n aggregation parameters	page 688
airtime-fairness	Enables fair access for clients based on airtime usage	page 690
antenna-diversity	Transmits antenna diversity for non-11n transmit rates	page 691
antenna-downtilt	Enables *Advanced Element Panel Technology* (ADEPT) antenna mode	page 691
antenna-gain	Specifies the antenna gain for the selected radio	page 692
antenna-mode	Configures the radio antenna mode	page 693
beacon	Configures beacon parameters	page 694
channel	Configures a radio's channel of operation	page 695
data-rates	Specifies the 802.11 rates supported on a radio	page 696
description	Configures the selected radio's description	page 700
dfs-rehome	Reverts to configured home channel once *Dynamic Frequency Selection* (DFS) evacuation period expires	page 701
dynamic-chain-selection	Enables automatic antenna mode selection	page 702
ekahau	Enables Ekahau multicast packet forwarding	page 702
extended-range	Configures extended range	page 703
guard-interval	Configures the 802.11n guard interval	page 704

Commands	Description	Reference
ldpc	Enables support for *Low Density Parity Check* (LDPC) on the radio interface	page 705
lock-rf-mode	Retains user configured RF mode settings for the selected radio	page 706
max-clients	Configures the maximum number of wireless clients allowed to associate with this radio	page 707
mesh	Configures radio mesh parameters	page 708
meshpoint	Maps an existing meshpoint to this radio interface	page 709
no	Negates or resets radio interface settings configures on a profile or a device	page 710
non-unicast	Configures the handling of non unicast frames on this radio	page 713
off-channel-scan	Enables selected radio's off channel scanning parameters	page 715
placement	Defines selected radio's deployment location	page 716
power	Configures the transmit power on this radio	page 717
preamble-short	Enables the use of short preamble on this radio	page 718
probe-response	Configures transmission parameters for probe response frames	page 719
radio-resource-measurement	Enables 802.11k radio resource measurement	page 720
radio-share-mode	Configures the mode of operation, for this radio, as radio-share	page 721
rate-selection	Sets the rate selection method to standard or opportunistic	page 722
remove-override	Removes the radio's channel of operation	page 723
rf-mode	Configures the radio's RF mode	page 723
rifs	Configures *Reduced Interframe Spacing* (RIFS) parameters on this radio	page 725
rts-threshold	Configures the *Request to Send* (RTS) threshold value on this radio	page 726
shutdown	Terminates or shuts down selected radio interface	page 727
sniffer-redirect	Captures and redirects packets to an IP address running a packet capture/analysis tool	page 727
stbc	Configures radio's *Space Time Block Coding* (STBC) mode	page 729
use	Enables use of an association ACL policy and a radio QoS policy by selected radio interface	page 729
wireless-client	Configures wireless client parameters on selected radio	page 731
wlan	Enables a WLAN on selected radio	page 732

aeroscout

interface-config-radio-instance

Enables Aeroscout multicast packet forwarding. This feature is disabled by default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
aeroscout [forward|mac <MAC>]
```

Parameters

```
aeroscout [forward|mac <MAC>]
```

forward	Enables Aeroscout multicast packet forwarding
mac <MAC>	Configures the multicast MAC address to forward the packets • <MAC> – Specify the MAC address in the AA-BB-CC-DD-EE-FF format.

Example

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#aeroscout forward

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  aeroscout forward
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands:

no	Disables Aeroscout Multicast packet forwarding

aggregation

interface-config-radio-instance

Configures 802.11n frame aggregation. Frame aggregation increases throughput by sending two or more data frames in a single transmission. There are two types of frame aggregation: *MAC Service Data Unit* (MSDU) aggregation and *MAC Protocol Data Unit* (MPDU) aggregation. Both modes group several data frames into one large data frame.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
aggregation [ampdu|amsdu]

aggregation ampdu [rx-only|tx-only|tx-rx|none|max-aggr-size|min-spacing]
aggregation ampdu [rx-only|tx-only|tx-rx|none]
aggregation ampdu max-aggr-size [rx|tx]
aggregation ampdu max-aggr-size rx [8191|16383|32767|65535]
aggregation ampdu max-aggr-size tx <2000-65535>
aggregation ampdu min-spacing [0|1|2|4|8|16]

aggregation amsdu [rx-only|tx-rx]
```

Parameters

```
aggregation ampdu [rx-only|tx-only|tx-rx|none]
```

aggregation	Configures 802.11n frame aggregation parameters
ampdu	Configures *Aggregate MAC Protocol Data Unit* (AMPDU) frame aggregation parameters AMPDU aggregation collects Ethernet frames addressed to a single destination. It wraps each frame in an 802.11n MAC header. This aggregation mode is less efficient, but more reliable in environments with high error rates. It enables the acknowledgement and retransmission of each aggregated data frame individually.

tx-only	Supports the transmission of AMPDU aggregated frames only
rx-only	Supports the receipt of AMPDU aggregated frames only
tx-rx	Supports the transmission and receipt of AMPDU aggregated frames (default setting)
none	Disables support for AMPDU aggregation

`aggregation ampdu max-aggr-size rx [8191|16383|32767|65535]`

aggregation	Configures 802.11n frame aggregation parameters
ampdu	Configures AMPDU frame aggregation parameters AMPDU aggregation collects Ethernet frames addressed to a single destination. It wraps each frame in an 802.11n MAC header. This aggregation mode is less efficient, but more reliable in environments with high error rates. It enables the acknowledgement and retransmission of each aggregated data frame individually.
max-aggr-size	Configures AMPDU packet size limits. Configure the packet size limit on packets both transmitted and received.
rx [8191|16383|32767|65535]	Configures the limit on received frames • 8191 – Advertises a maximum of 8191 bytes • 16383 – Advertises a maximum of 16383 bytes • 32767 – Advertises a maximum of 32767 bytes • 65535 – Advertises a maximum of 65535 bytes (default setting)

`aggregation ampdu max-aggr-size tx <2000-65535>`

aggregation	Configures 802.11n frame aggregation parameters
ampdu	Configures AMPDU frame aggregation parameters AMPDU aggregation collects Ethernet frames addressed to a single destination. It wraps each frame in an 802.11n MAC header. This aggregation mode is less efficient, but more reliable in environments with high error rates. It enables the acknowledgement and retransmission of each aggregated data frame individually.
max-aggr-size	Configures AMPDU packet size limits. Configure the packet size limit on packets both transmitted and received.
tx <2000-65535>	Configures the maximum size (in bytes) for AMPDU aggregated transmitted frames • <2000-65535> – Sets the limit from 2000 - 65535 bytes. The default is 65535 bytes.

`aggregation ampdu min-spacing [0|1|2|4|8|16]`

aggregation	Configures 802.11n frame aggregation parameters
ampdu	Configures AMPDU frame aggregation parameters AMPDU aggregation collects Ethernet frames addressed to a single destination. It wraps each frame in an 802.11n MAC header. This aggregation mode is less efficient, but more reliable in environments with high error rates. It enables the acknowledgement and retransmission of each aggregated data frame individually.
mn-spacing [0|1|2|4|8|16]	Configures the minimum gap, in microseconds, between AMPDU frames • 0 – Configures the minimum gap as 0 microseconds • 1 – Configures the minimum gap as 1 microseconds • 2 – Configures the minimum gap as 2 microseconds • 4 – Configures the minimum gap as 4 microseconds (default setting) • 8 – Configures the minimum gap as 8 microseconds • 16 – Configures the minimum gap as 16 microseconds

```
aggregation amsdu [rx-only|tx-rx]
```

aggregation	Configures 802.11n frame aggregation parameters
amsdu	Configures *Aggregated MAC Service Data Unit* (AMSDU) frame aggregation parameters. AMSDU aggregation collects Ethernet frames addressed to a single destination. But, unlike AMPDU, it wraps all frames in a single 802.11n frame.
rx-only	Supports the receipt of AMSDU aggregated frames only (default setting)
tx-rx	Supports the transmission and receipt of AMSDU aggregated frames

Example

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#aggregation ampdu
tx-only

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  aggregation ampdu tx-only
  aeroscout forward
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands:

no	Disables 802.11n aggregation parameters

airtime-fairness

interface-config-radio-instance

Enables equal access for wireless clients based on their airtime usage

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
airtime-fairness {prefer-ht} {weight <1-10>}
```

Parameters

```
airtime-fairness {prefer-ht} {weight <1-10>}
```

airtime-fairness	Enables equal access for wireless clients based on their airtime usage
prefer-ht	Optional. Gives preference to high throughput (802.11n) clients over legacy clients
weight <1-10>	Optional. Configures the relative weightage for 11n clients over legacy clients. • <1-10> – Sets a weightage ratio for 11n clients from 1 - 10

Example

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#airtime-fairness
prefer-ht weight 6

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  aggregation ampdu tx-only
  aeroscout forward
  airtime-fairness prefer-ht weight 6
```

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands:

no	Disables fair access for wireless clients (provides access on a round-robin mode)

antenna-diversity

interface-config-radio-instance

Configures transmit antenna diversity for non-11n transmit rates

Antenna diversity uses two or more antennas to increase signal quality and strength. This option is disabled by default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
antenna-diversity
```

Parameters

None

Example

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#antenna-diversity

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  aggregation ampdu tx-only
  aeroscout forward
  antenna-diversity
  airtime-fairness prefer-ht weight 6
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands:

no	Uses single antenna for non-11n transmit rates

antenna-downtilt

interface-config-radio-instance

Enables the *Advanced Element Panel Technology* (ADEPT) antenna mode. The ADEPT mode increases the probability of parallel data paths enabling multiple spatial data streams. This option is disabled by default.

Supported in the following platforms:

- Access Point — Brocade Mobility 71XX Access Point

NOTE
This feature is not supported on Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, and Brocade Mobility 1220 Access Point.

Syntax:

```
antenna-downtilt
```

Parameters

None

Example

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#antenna-downtilt

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  antenna-gain 12.0
  aggregation ampdu tx-only
  aeroscout forward
  antenna-diversity
  airtime-fairness prefer-ht weight 6
  antenna-downtilt
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands:

no	Disables the ADEPT antenna mode

antenna-gain

interface-config-radio-instance

Configures the antenna gain for the selected radio

Antenna gain is the ability of an antenna to convert power into radio waves and vice versa. The access point or wireless controller's *Power Management Antenna Configuration File* (PMACF) automatically configures the access point orwireless controller's radio transmit power based on the antenna type, its antenna gain (provided here) and the deployed country's regulatory domain restrictions. Once provided, the access point or wireless controller calculates the power range. Antenna gain relates the intensity of an antenna in a given direction to the intensity that would be produced ideally by an antenna that radiates equally in all directions (isotropically), and has no losses. Although the gain of an antenna is directly related to its directivity, its gain is a measure that takes into account the efficiency of the antenna as well as its directional capabilities. Brocade recommends that only a professional installer set the antenna gain.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
antenna-gain <0.0-15.0>
```

Parameters

```
antenna-gain <0.0-15.0>
```

<0.0-15.0>	Sets the antenna gain from 0.0 - 15.0 dBi. The default 0.00.

Example

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#antenna-gain 12.0

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  antenna-gain 12.0
  aggregation ampdu tx-only
  aeroscout forward
  antenna-diversity
  airtime-fairness prefer-ht weight 6
  antenna-downtilt
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands:

no	Resets the radio's antenna gain parameter

antenna-mode

interface-config-radio-instance

Configures the antenna mode (the number of transmit and receive antennas) on the radio

This command sets the number of transmit and receive antennas on the access point. The 1x1 mode is used for transmissions over just the single -A- antenna, 1xALL is used for transmissions over the -A- antenna and all three antennas for receiving. The 2x2 mode is used for transmissions and receipts over two antennas for dual antenna models. The default setting is dynamic based on the access point model deployed and its transmit power settings.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
antenna-mode [1*1|1*ALL|2*2|default]
```

Parameters

```
antenna-mode [1*1|1*ALL|2*2|default]
```

1*1	Uses only antenna A to receive and transmit
1*ALL	Uses antenna A to transmit and receives on all antennas
2*2	Uses antenna A and C for both transmit and receive
default	Uses default antenna settings. This is the default setting.

Usage Guidelines:

To support STBC feature on Brocade Mobility 71XX Access Point profile, the antenna-mode should not be configured to 1x1.

Example

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#antenna-mode 2x2

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
```

```
 interface radio1
  antenna-gain 12.0
  aggregation ampdu tx-only
  aeroscout forward
  antenna-mode 2x2
  antenna-diversity
  airtime-fairness prefer-ht weight 6
  antenna-downtilt
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands:

no	Resets the radio antenna mode (the number of transmit and receive antennas) to its default

beacon

interface-config-radio-instance

Configures radio beacon parameters

A beacon is a packet broadcasted by adopted radios to keep the network synchronized. Included in a beacon is information, such as the WLAN service area, the radio address, the broadcast destination addresses, a time stamp, and indicators about traffic and delivery such as a *Delivery Traffic Indication Message* (DTIM). Increase the DTIM/beacon settings (lengthening the time) to let nodes sleep longer and preserve battery life. Decrease these settings (shortening the time) to support streaming-multicast audio and video applications that are jitter sensitive.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
beacon [dtim-period|period]
beacon dtim-period [<1-50>|bss]
beacon dtim-period [<1-50>|bss <1-16> <1-50>]
beacon period [50|100|200]
```

Parametersd

```
beacon dtim-period [<1-50>|bss <1-8> <1-50>]
```

beacon	Configures radio beacon parameters
dtim-period	Configures the radio DTIM interval. A DTIM is a message that informs wireless clients about the presence of buffered multicast or broadcast data. The message is generated within the periodic beacon at a frequency specified by the DTIM interval.
<1-50>	Configures a single value to use on the radio. Specify a value between 1 and 50.
bss <1-16> <1-50>	Configures a separate DTIM for a *Basic Service Set* (BSS) on a radio • <1-16> – Sets the BSS number from 1 - 16 • <1-50> – Sets the BSS DTIM from 1 - 50

```
beacon period [50|100|200]
```

period [50|100|200]	Configures the beacon period (the interval between consecutive radio beacons) • 50 – Configures 50 K-uSec interval between beacons • 100 – Configures 100 K-uSec interval between beacons (default) • 200 – Configures 200 K-uSec interval between beacons

Example

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#beacon dtim-period
bss 2 20
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#beacon period 50

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  beacon period 50
  beacon dtim-period bss 1 2
  beacon dtim-period bss 2 20
  beacon dtim-period bss 3 2
  --More--
```

Related Commands:

no	Removes the configured beacon parameters

channel

interface-config-radio-instance

Configures a radio's channel of operation

Only a trained installation professional should define the radio channel. Select Smart for the radio to scan non-overlapping channels listening for beacons from other access points. After the channels are scanned, the radio selects the channel with the fewest access points. In case of multiple access points on the same channel, it selects the channel with the lowest average power level.

NOTE
Channels with a "w" appended to them are unique to the 40 MHz band. Channels with a "ww" appended to them are 802.11ac specific, and appear only when using an AP8232, and are unique to the 80 MHz band.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
channel [smart|acs|1|2|3|4|-------]
```

Parameters

```
channel [smart|acs|1|2|3|4|-------]
```

smart|acs|1|2|3|4|------]	Configures a radio's channel of operation. The options are: • smart – Uses Smart RF to assign a channel (uses uniform spectrum spreading if Smart RF is not enabled). This is the default setting. • acs – Uses *automatic channel selection* (ACS) to assign a channel • 1 – Channel 1 in 20 MHz • 2 – Channel 1 in 20 MHz

Example

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#channel 1

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  channel 1
  beacon period 50
  beacon dtim-period bss 1 5
  beacon dtim-period bss 2 2
  ......................................
  beacon dtim-period bss 14 5
  beacon dtim-period bss 15 5
  beacon dtim-period bss 16 5
  antenna-gain 12.0
  aggregation ampdu tx-only
  aeroscout forward
  antenna-mode 2x2
  antenna-diversity
--More--
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands:

no	Resets a radio's channel of operation

data-rates

interface-config-radio-instance

Configures the 802.11 data rates on this radio

This command sets the rate options depending on the 802.11 protocol and the radio band selected. If 2.4 GHz is selected as the radio band, select separate 802.11b, 802.11g and 802.11n rates and define how they are used in combination. If 5.0 GHz is selected as the radio band, select separate 802.11a and 802.11n rates then define how they are used together.

If dedicating the radio to either 2.4 or 5.0 GHz support, use the *custom* keyword to set a 802.11n *modulation and coding scheme* (MCS) in respect to the radio's channel width and guard interval. A MCS defines (based on RF channel conditions) an optimal combination of rates, bonded channels, multiple spatial streams, different guard intervals and modulation types. Clients can associate as long as they support basic MCS (as well as non-11n basic rates).

Data rates are fixed and not user configurable for radios functioning as sensors.

NOTE
Use the rf-mode command to configure a radio's mode of operation.

NOTE
The MCS-1s and MCS-2s options are available for each supported access point.

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
data-rates [b-only|g-only|a-only|bg|bgn|gn|an|default|custom|mcs]

data-rates [b-only|g-only|a-only|bg|bgn|gn|an|default]

data-rates custom
[1|2|5.5|6|9|11|12|18|24|36|48|54|mcs-1s|mcs-2s|mcs-3s|basic-1|

basic-2|basic-5.5|basic-6|basic-9|basic-11|basic-12|basic-18|basic-24|basic-3
6|
          basic-48|basic-54|basic-mcs-1s]

data-rates mcs qam-only
```

Parameters

`data-rates [b-only|g-only|a-only|bg|bgn|gn|an|default]`

b-only	Supports operation in the 802.11b mode only (applicable for 2.4 and 4.9 GHz bands)
g-only	Uses rates that support operation in the 802.11g mode only (applicable for 2.4 and 4.9 GHz bands)
a-only	Uses rates that support operation in the 802.11a mode only (applicable for 5.0 GHz band only)
bg	Uses rates that support 802.11b and 802.11g wireless clients (applicable for 2.4 and 4.9 GHz bands)
bgn	Uses rates that support 802.11b, 802.11g, and 802.11n wireless clients (applicable for 2.4 and 4.9 GHz bands)
gn	Uses rates that support 802.11g and 802.11n wireless clients (applicable for 2.4 and 4.9 GHz bands)
an	Uses rates that support 802.11a and 802.11n wireless clients (applicable for 5.0 GHz band only)
default	Enables the default data rates according to the radio's band of operation

```
data-rates custom
[1|2|5.5|6|9|11|12|18|24|36|48|54||mcs-1s|mcs-2s|mcs-3s|basic-1|
basic-2|basic-5.5|basic-6|basic-9|basic-11|basic-12|basic-18|basic-24|basic-3
6|
basic-48|basic-54|basic-mcs-1s]
```

custom	Configures a list of data rates by specifying each rate individually. Use 'basic-' prefix before a rate to indicate it's used as a basic rate (For example, 'data-rates custom basic-1 basic-2 5.5 11') • 1 – 1-Mbps • 2 – 2-Mbps • 5.5 – 5.5-Mbps • 6 – 6-Mbps • 9 – 9-Mbps • 11 – 11-Mbps • 12 – 12-Mbps • 18 – 18-Mbps • 24 – 24-Mbps • 36 – 36-Mbps • 48 – 48-Mbps • 54 – 54-Mbps • mcs-1s – Applicable to 1-spatial stream data rates • mcs-2s – Applicable to 2-spatial stream data rates • basic-1 – Basic 1-Mbps • basic-2 – Basic 2-Mbps • basic-5.5 – Basic 5.5-Mbps • basic-6 – Basic 6-Mbps • basic-9 – Basic 9-Mbps • basic-11 – Basic 11-Mbps • basic-12 – Basic 12-Mbps • basic-18 – Basic 18-Mbps • basic-24 – Basic 24-Mbps • basic-36 – Basic 36-Mbps • basic-48 – Basic 48-Mbps • basic-54 – Basic 54-Mbps • basic-mcs-1s – Modulation and Coding Scheme data rates for 1 Spatial Stream Refer to the *Usage Guidelines (Supported data rates)* section for 802.11an and 802.11ac MCS detailed dates rates for both with and without *short guard intervals* (SGI).

```
data-rates mcs qam-only
```

mcs qam-only	Configures supports for MCS QAM data rates only

Usage Guidelines: (Supported data rates)

The following table defines the 802.11n MCS for MCS 1 streams, both with and without SGI:

MCS-1Stream Index	Number of Streams	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	20 MHz With SGI
0	1	6.5	7.2	13.5	15
1	1	13	14.4	27	30
2	1	19.5	21.7	40.5	45
3	1	26	28.9	54	60
4	1	39	43.4	81	90
5	1	52	57.8	108	120

MCS-1Stream Index	Number of Streams	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	20 MHz With SGI
6	1	58.5	65	121.5	135
7	1	65	72.2	135	150

The following table defines the 802.11n MCS for MCS 2 streams, both with and without SGI:

MCS-2Stream Index	Number of Streams	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	20 MHz With SGI
0	2	13	14.4	27	30
1	2	26	28.9	54	60
2	2	39	43.4	81	90
3	2	52	57.8	108	120
4	2	78	86.7	162	180
5	2	104	115.6	216	240
6	2	117	130	243	270
7	2	130	144.4	270	300

The following table defines the 802.11n MCS for MCS 3 streams, both with and without SGI:

MCS-3Stream Index	Number of Streams	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	20 MHz With SGI
0	3	19.5	21.7	40.5	45
1	3	39	43.3	81	90
2	3	58.5	65	121.5	135
3	3	78	86.7	162	180
4	3	117	130.7	243	270
5	3	156	173.3	324	360
6	3	175.5	195	364.5	405
7	3	195	216.7	405	450

The following table defines the 802.11ac MCS rates (theoretical throughput for single spatial streams) both with and without SGI:

MCS Index	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	40 MHz With SGI	80 MHz No SGI	80 MHz No SGI
0	6.5	7.2	13.5	15	29.3	32.5
1	13	14.4	27	30	58.5	65
2	19.5	21.7	40.5	45	87.8	97.5
3	26	28.9	54	60	117	130
4	39	43.3	81	90	175.5	195
5	52	57.8	108	120	234	260
6	58.5	65	121.5	135	263.3	292.5
7	65	72.2	135	150	292,5	325

MCS Index	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	40 MHz With SGI	80 MHz No SGI	80 MHz No SGI
8	78	86.7	162	180	351	390
9	N/A	N/A	180	200	390	433.3

Example

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#data-rates b-only

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  channel 1
  data-rates b-only
  beacon period 50
  beacon dtim-period bss 1 5
  beacon dtim-period bss 2 2
  beacon dtim-period bss 3 5
  ..................................................
  beacon dtim-period bss 13 5
  beacon dtim-period bss 14 5
  beacon dtim-period bss 15 5
  beacon dtim-period bss 16 5
  antenna-gain 12.0
  aggregation ampdu tx-only
  aeroscout forward
  --More--
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands:

no	Resets the 802.11 data rates on a radio
rf-mode	Configures the radio's RF mode of operation

description

interface-config-radio-instance

Configures the selected radio's description

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
description <WORD>
```

Parameters

```
description <WORD>
```

<WORD>	Defines a description for the selected radio (should not exceed 64 characters in length)

Example

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#description "Primary
radio to use"
```

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  description Primary\ radio\ to\ use
  channel 1
  data-rates b-only
  beacon period 50
  beacon dtim-period bss 1 5
  beacon dtim-period bss 2 2
  beacon dtim-period bss 3 5
  beacon dtim-period bss 4 5
  beacon dtim-period bss 5 5
  beacon dtim-period bss 6 5
  beacon dtim-period bss 7 5
  beacon dtim-period bss 8 5
  beacon dtim-period bss 9 5
  beacon dtim-period bss 10 5
  beacon dtim-period bss 11 5
  beacon dtim-period bss 12 5
  beacon dtim-period bss 13 5
  beacon dtim-period bss 14 5
  beacon dtim-period bss 15 5
  beacon dtim-period bss 16 5
  antenna-gain 12.0
  aggregation ampdu tx-only
--More--
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands:

no	Removes a radio's description

dfs-rehome

interface-config-radio-instance

Reverts to configured home channel once the *Dynamic Frequency Selection* (DFS) evacuation period expires

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
dfs-rehome
```

Parameters

None

Example

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#dfs-rehome
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands:

no	Stays on DFS elected channel after evacuation period expires

dynamic-chain-selection

interface-config-radio-instance

Enables automatic antenna mode selection (single antenna for non-11n transmit rates). This option is enabled by default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
dynamic-chain-selection
```

Parameters

None

Example

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#dynamic-chain-select
ion
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands:

no	Uses the configured transmit antenna mode for all clients

ekahau

interface-config-radio-instance

Enables Ekahau multicast packet forwarding

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
ekahau [forward|mac <MAC>]
ekahau forward ip <IP> port <0-65535>
```

Parameters

```
ekahau [forward|mac <MAC>]
```

forward ip <IP> port <0-65535>	Enables multicast packet forwarding to the Ekahau engine • ip <IP> – Configures the IP address of the Ekahau engine in the A.B.C.D format • port <0-65535> – Specifies the *TaZman Sniffer Protocol* (TZSP) port on Ekahau engine from 0 - 65535 TZSP is an encapsulation protocol, which is generally used to wrap 802.11 wireless packets.
mac <MAC>	Configures the multicast MAC address to forward the packets • <MAC> – Specify the MAC address in the AA-BB-CC-DD-EE-FF format.

Example

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#ekahau forward ip
172.16.10.1 port 3

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  description Primary\ radio\ to\ use
  channel 1
  data-rates b-only
  beacon period 50
  beacon dtim-period bss 1 5
  beacon dtim-period bss 2 2
  beacon dtim-period bss 3 5
  beacon dtim-period bss 4 5
  beacon dtim-period bss 5 5
  beacon dtim-period bss 6 5
  beacon dtim-period bss 7 5
  beacon dtim-period bss 8 5
  beacon dtim-period bss 9 5
  beacon dtim-period bss 10 5
  beacon dtim-period bss 11 5
  beacon dtim-period bss 12 5
  beacon dtim-period bss 13 5
  beacon dtim-period bss 14 5
  beacon dtim-period bss 15 5
  beacon dtim-period bss 16 5
  antenna-gain 12.0
  aggregation ampdu tx-only
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  antenna-mode 2x2
--More--
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands:

no	Uses default Ekahau multicast MAC address

extended-range

interface-config-radio-instance

Configures the extended range capability for Brocade Mobility 71XX Access Point model devices

Supported in the following platforms:

- Access Point — Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
extended-range <1-25>
```

Parameters

```
extended-range <1-25>
```

extended-range <1-25>	Configures extended range on this radio interface from 1 - 25 kilometers. The default is 2 km on 2.4 GHz band and 7 km on 5.0 GHz band.

Example

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#extended-range

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  description Primary\ radio\ to\ use
  channel 1
  data-rates b-only
  beacon period 50
  beacon dtim-period bss 1 5
  beacon dtim-period bss 2 2
  beacon dtim-period bss 3 5
  beacon dtim-period bss 4 5
  beacon dtim-period bss 5 5
  beacon dtim-period bss 6 5
  beacon dtim-period bss 7 5
  beacon dtim-period bss 8 5
  beacon dtim-period bss 9 5
  beacon dtim-period bss 10 5
  beacon dtim-period bss 11 5
  beacon dtim-period bss 12 5
  beacon dtim-period bss 13 5
  beacon dtim-period bss 14 5
  beacon dtim-period bss 15 5
  beacon dtim-period bss 16 5
  antenna-gain 12.0
  aggregation ampdu tx-only
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  antenna-mode 2x2
  antenna-diversity
  airtime-fairness prefer-ht weight 6
  extended-range 15
--More--
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands:

no	Resets the extended range to default (7 km for 2.4 GHz and 5 km for 5.0 GHz)

guard-interval

interface-config-radio-instance

Configures the 802.11n guard interval. A guard interval ensures distinct transmissions do not interfere with one another. It provides immunity to propagation delays, echoes and reflection of radio signals.

The guard interval is the space between transmitted characters. The guard interval eliminates *inter symbol interference* (ISI). ISI which occurs when echoes or reflections from one symbol interferes with another. Adding time between transmissions allows echoes and reflections to settle before the next symbol is transmitted. A shorter guard interval results in shorter symbol times, which reduces overhead and increases data rates by up to 10%.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
guard-interval [any|long]
```

Parameters

```
guard-interval [any|long]
```

any	Enables the radio to use any short (400nSec) or long (800nSec) guard interval
long	Enables the use of long guard interval (800nSec). This is the default setting.

Example

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#guard-interval long

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  description Primary\ radio\ to\ use
  channel 1
  data-rates b-only
  beacon period 50
  beacon dtim-period bss 1 5
  beacon dtim-period bss 2 2
  beacon dtim-period bss 3 5
  beacon dtim-period bss 4 5
  beacon dtim-period bss 5 5
  beacon dtim-period bss 6 5
  beacon dtim-period bss 7 5
  beacon dtim-period bss 8 5
  beacon dtim-period bss 9 5
  beacon dtim-period bss 10 5
  beacon dtim-period bss 11 5
  beacon dtim-period bss 12 5
  beacon dtim-period bss 13 5
  beacon dtim-period bss 14 5
  beacon dtim-period bss 15 5
  beacon dtim-period bss 16 5
  antenna-gain 12.0
  guard-interval long
--More--
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands:

no	Resets the 802.11n guard interval to default (long: 800nSec)

ldpc

interface-config-radio-instance

Enables support for *Low Density Parity Check* (LDPC) on the radio interface.

LDPC consists of forward error correcting codes that enable error control in data transmission.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
ldpc
```

Parameters

None

Example

```
rfs4000-229D58(config-profile-Test81XX-if-radio1)#ldpc
rfs4000-229D58(config-profile-Test81XX-if-radio1)#

rfs4000-229D58(config-profile-Test81XX-if-radio1)#show context
 interface radio1
  ldpc
rfs4000-229D58(config-profile-Test81XX-if-radio1)#
```

Related Commands:

no	Disables LDPC support

lock-rf-mode

interface-config-radio-instance

Retains user configured RF mode settings for the selected radio

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
lock-rf-mode
```

Parameters

None

Example

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#lock-rf-mode

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  description Primary\ radio\ to\ use
  channel 1
  data-rates b-only
  beacon period 50
  beacon dtim-period bss 1 5
  beacon dtim-period bss 2 2
  beacon dtim-period bss 3 5
  beacon dtim-period bss 4 5
  beacon dtim-period bss 5 5
  beacon dtim-period bss 6 5
  beacon dtim-period bss 7 5
  beacon dtim-period bss 8 5
  beacon dtim-period bss 9 5
  beacon dtim-period bss 10 5
```

```
  beacon dtim-period bss 11 5
  beacon dtim-period bss 12 5
  beacon dtim-period bss 13 5
  beacon dtim-period bss 14 5
  beacon dtim-period bss 15 5
  beacon dtim-period bss 16 5
  antenna-gain 12.0
  guard-interval long
  aggregation ampdu tx-only
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  antenna-mode 2x2
  antenna-diversity
  airtime-fairness prefer-ht weight 6
  lock-rf-mode
  extended-range 15
--More--
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands:

no	Allows Smart RF to change a radio's RF mode settings

max-clients

interface-config-radio-instance

Configures the maximum number of wireless clients allowed to associate with this radio

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
max-clients <0-256>
```

Parameters

```
max-clients <0-256>
```

<0-256>	Configures the maximum number of clients allowed to associate with a radio. Specify a value from 0 - 256. The default is 256.

Example

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#max-clients 100

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  description Primary\ radio\ to\ use
  channel 1
  data-rates b-only
  beacon period 50
  beacon dtim-period bss 1 5
  beacon dtim-period bss 2 2
  ..........................................
  beacon dtim-period bss 12 5
  beacon dtim-period bss 13 5
```

```
  beacon dtim-period bss 14 5
  beacon dtim-period bss 15 5
  beacon dtim-period bss 16 5
  antenna-gain 12.0
  guard-interval long
  aggregation ampdu tx-only
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  antenna-mode 2x2
  antenna-diversity
  max-clients 100
  airtime-fairness prefer-ht weight 6
  lock-rf-mode
  extended-range 15
  antenna-downtilt
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands:

no	Resets the maximum number of wireless clients allowed to associate with a radio

mesh

interface-config-radio-instance

Use this command to configure radio mesh parameters. A *Wireless Mesh Network* (WMN) is a network of radio nodes organized in a mesh topology. It consists of mesh clients, mesh routers, and gateways.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
mesh [client|links|portal|preferred-peer|psk]

mesh [client|links <1-6>|portal|preferred-peer <1-6> <MAC>|psk [0 <LINE>|2
<LINE>|
          <LINE>]]
```

Parameters

```
mesh [client|links <1-6>|portal|preferred-peer <1-6> <MAC>|psk [0 <LINE>|2
<LINE>|
<LINE>]]
```

mesh	Configures radio mesh parameters, such as maximum number of mesh links, preferred peer device, client operations etc.
client	Enables operation as a client (scans for mesh portals or nodes that have connectivity to portals and connects through them) Setting the mesh mode to ‘client’ enables the radio to operate as a mesh client that scans for and connects to mesh portals or nodes that are connected to portals.
links <1-6>	Configures the maximum number of mesh links a radio attempts to create • <1-6> – Sets the maximum number of mesh links from 1 - 6. The default is 3.

portal	Enables operation as a portal (begins beaconing immediately, accepting connections from other mesh nodes, typically the node with a connection to the wired network) Setting the mesh mode to 'portal' turns the radio into a mesh portal. The radio starts beaconing immediately and accepts connections from other mesh nodes.
preferred-peer <1-6> <MAC>	Configures a preferred peer device • <1-6> – Configures the priority at which the peer node will be added When connecting to the mesh infrastructure, nodes with lower priority are given precedence over nodes with higher priority. • <MAC> – Sets the MAC address of the preferred peer device (Ethernet MAC of either a AP, wireless controller, or service platform with onboard radios)
psk [0 <LINE>|2 <LINE>|<LINE>]	Configures the pre-shared key • 0 <LINE> – Enter a clear text key • 2 <LINE> – Enter an encrypted key • <LINE> – Enter the pre-shared key Pre-shared keys should be 8 - 64 characters in length.

Example

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#mesh client

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  description Primary\ radio\ to\ use
  channel 1
  data-rates b-only
  mesh client
  beacon period 50
  --More--
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands:

no	Disables mesh mode operation of the selected radio

meshpoint

interface-config-radio-instance

Maps an existing meshpoint to this radio

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
meshpoint <MESHPOINT-NAME> {bss <1-16>}
```

Parameters

```
meshpoint <MESHPOINT-NAME> {bss <1-16>}
```

meshpoint <MESHPOINT-NAME>	Maps a meshpoint to this radio. Specify the meshpoint name.
bss <1-16>	Optional. Specifies the radio's BSS where this meshpoint is mapped • <1-16> – Specify the BSS number from 1 - 16.

Example

```
rfs7000-37FABE(config-profile-ap71xxTest-if-radio1)#meshpoint test bss 7
rfs7000-37FABE(config-profile-ap71xxTest-if-radio1)#show context
 interface radio1
  meshpoint test bss 7
rfs7000-37FABE(config-profile-ap71xxTest-radio1)#
```

Related Commands:

no	Disables meshpoint on the selected radio

no

interface-config-radio-instance

Negates a command or resets settings to their default. When used in the profile/device > radio interface configuration mode, the no command disables or resets radio interface settings.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
no <PARAMETER>
```

Parameters

None

Usage Guidelines:

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
rfs7000-37FABE(config-profile-ap71xxTest-if-radio1)#no ?
  aeroscout                  Use Default Aeroscout Multicast MAC Address
  aggregation                Configure 802.11n aggregation related parameters
  airtime-fairness           Disable fair access to medium for clients,
                             provide access in a round-robin mode
  antenna-diversity          Use single antenna for non-11n transmit rates
  antenna-downtilt           Reset ADEPT antenna mode
  antenna-gain               Reset the antenna gain of this radio to default
  antenna-mode               Reset the antenna mode (number of transmit and
                             receive antennas) on the radio to its default
  association-list           Configure the association list for the radio
  beacon                     Configure beacon parameters
  channel                    Reset the channel of operation of this radio to
                             default
```

```
  data-rates                  Reset radio data rate configuration to default
  description                 Reset the description of the radio to its
                              default
  dfs-rehome                  Stay on dfs elected channel after evacuation
                              period expires
  dynamic-chain-selection     Use the configured transmit antenna mode for all
                              clients
  ekahau                      Use Default Ekahau Multicast MAC Address
  extended-range              Reset extended range to default
  guard-interval              Configure default value of 802.11n guard
                              interval (long: 800nSec)
  ldpc                        Configure support for Low Density Parity Check
                              Code
  lock-rf-mode                Allow smart-rf to change rf-mode setting for
                              this radio
  max-clients                 Maximum number of wireless clients allowed to
                              associate
  mesh                        Disable mesh mode operation of the radio
  meshpoint                   Disable a meshpoint from this radio
  non-unicast                 Configure handling of non-unicast frames
  off-channel-scan            Disable off-channel scanning on the radio
  placement                   Reset the placement of the radio to its default
  power                       Reset the transmit power of this radio to
                              default
  preamble-short              Disable the use of short-preamble on this radio
  probe-response              Configure transmission parameters for Probe
                              Response frames
  radio-resource-measurement  Configure support for 802.11k Radio Resource
                              Measurement
  radio-share-mode            Configure the radio-share mode of operation for
                              this radio
  rate-selection              Monotonic rate selection
  rf-mode                     Reset the RF mode of operation for this radio to
                              default (2.4GHz on radio1, 5GHz on radio2,
                              sensor on radio3)
  rifs                        Configure Reduced Interframe Spacing (RIFS)
                              parameters
  rts-threshold               Reset the RTS threshold to its default (65536)
  shutdown                    Re-enable the selected interface
  sniffer-redirect            Disable capture and redirection of packets
  stbc                        Configure Space-Time Block Coding (STBC)
                              parameters

  use                         Set setting to use
  wireless-client             Configure wireless client related parameters
  wlan                        Disable a wlan from this radio

  service                     Service Commands

rfs7000-37FABE(config-profile-ap71xxTest-if-radio1)#
```

The following example shows radio interface settings before the ‘no’ commands are executed:

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  description Primary\ radio\ to\ use
  channel 1
  data-rates b-only
  mesh client
```

```
  beacon period 50
  beacon dtim-period bss 1 5
  beacon dtim-period bss 2 2
  beacon dtim-period bss 3 5
  beacon dtim-period bss 4 5
  beacon dtim-period bss 5 5
  beacon dtim-period bss 6 5
  beacon dtim-period bss 7 5
  beacon dtim-period bss 8 5
  beacon dtim-period bss 9 5
  beacon dtim-period bss 10 5
  beacon dtim-period bss 11 5
  beacon dtim-period bss 12 5
  beacon dtim-period bss 13 5
  beacon dtim-period bss 14 5
  beacon dtim-period bss 15 5
  beacon dtim-period bss 16 5
  antenna-gain 12.0
  guard-interval long
  aggregation ampdu tx-only
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  antenna-mode 2x2
  antenna-diversity
  max-clients 100
  airtime-fairness prefer-ht weight 6
  lock-rf-mode
  extended-range 15
  antenna-downtilt
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#no channel
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#no antenna-gain
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#no description
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#no antenna-mode
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#no beacon
dtim-period
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#no beacon period

The following example shows radio interface settings after the ‘no’ commands
are executed:

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  data-rates b-only
  mesh client
  guard-interval long
  aggregation ampdu tx-only
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  antenna-diversity
  max-clients 100
  airtime-fairness prefer-ht weight 6
  lock-rf-mode
  extended-range 15
  antenna-downtilt
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

non-unicast

interface-config-radio-instance

Configures the support for non unicast frames on this radio. Enables the forwarding of multicast and broadcast frames by this radio.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
non-unicast [forwarding|queue|tx-rate]

non-unicast forwarding [follow-dtim|power-save-aware]
non-unicast queue [<1-200>|bss]
non-unicast queue [<1-200>|bss <1-16> <1-200>]
non-unicast tx-rate [bss
<1-16>|dynamic-all|dynamic-basic|highest-basic|lowest-basic]
non-unicast tx-rate bss <1-16> [dynamic-all|dynamic-basic|highest-basic|
          lowest-basic]
```

Parameters

`non-unicast forwarding [follow-dtim|power-save-aware]`

non-unicast	Configures support for non unicast frames
forwarding	Configures multicast and broadcast frame forwarding on this radio
follow-dtim	Specifies frames always wait for the DTIM interval to time out. The DTIM interval is configured using the beacon command. This is the default setting.
power-save-aware	Enables immediate forwarding of frames if all associated wireless clients are in the power save mode

`non-unicast queue [<1-200>|bss <1-16> <1-200>]`

non-unicast	Configures support for non unicast frames
queue	Configures the number of broadcast packets queued per BSS on this radio. This command also enables you to override the default on a specific BSS.
<1-200>	Specify a number from 1 - 200.
bss <1-16> <1-200>	Overrides the default on a specified BSS • <1-16> – Select the BSS to override the default. • <1-200> – Specify the number of broadcast packets queued for the selected BSS.

`non-unicast tx-rate [bss <1-16>|dynamic-all|dynamic-basic|highest-basic|lowest-basic]`

non-unicast	Configures support for non unicast frames
tx-rate	Configures the transmission data rate for broadcast and multicast frames
bss <1-16>	Overrides the default on a specified BSS • <1-16> – Select the BSS to override the default.
dynamic-all	Dynamically selects a rate from all supported rates based on current traffic conditions
dynamic-basic	Dynamically selects a rate from all supported basic rates based on current traffic conditions

highest-basic	Uses the highest configured basic rate
lowest-basic	Uses the lowest configured basic rate

Example

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#non-unicast queue
bss 2 3

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#non-unicast tx-rate
bss 1 dynamic-all

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  data-rates b-only
  mesh client
  guard-interval long
  aggregation ampdu tx-only
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  non-unicast tx-rate bss 1 dynamic-all
  non-unicast tx-rate bss 2 highest-basic
  non-unicast tx-rate bss 3 highest-basic
  non-unicast tx-rate bss 4 highest-basic
  non-unicast tx-rate bss 5 highest-basic
  non-unicast tx-rate bss 6 highest-basic
  non-unicast tx-rate bss 7 highest-basic
  non-unicast tx-rate bss 8 highest-basic
  non-unicast tx-rate bss 9 highest-basic
  non-unicast tx-rate bss 10 highest-basic
  non-unicast tx-rate bss 11 highest-basic
  non-unicast tx-rate bss 12 highest-basic
  non-unicast tx-rate bss 13 highest-basic
  non-unicast tx-rate bss 14 highest-basic
  non-unicast tx-rate bss 15 highest-basic
  non-unicast tx-rate bss 16 highest-basic
  non-unicast queue bss 1 50
  non-unicast queue bss 2 3
  non-unicast queue bss 3 50
  non-unicast queue bss 4 50
  non-unicast queue bss 5 50
  non-unicast queue bss 6 50
  non-unicast queue bss 7 50
  non-unicast queue bss 8 50
  non-unicast queue bss 9 50
  non-unicast queue bss 10 50
  non-unicast queue bss 11 50
  non-unicast queue bss 12 50
  non-unicast queue bss 13 50
  non-unicast queue bss 14 50
  non-unicast queue bss 15 50
  non-unicast queue bss 16 50
  antenna-diversity
  max-clients 100
  airtime-fairness prefer-ht weight 6
  lock-rf-mode
  extended-range 15
  antenna-downtilt
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands:

no	Resets the handling of non unicast frames to its default

off-channel-scan

interface-config-radio-instance

Enables selected radio's off channel scanning parameters. This option is disabled by default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
off-channel-scan {channel-list|max-multicast|scan-interval|sniffer-redirect}

off-channel-scan {channel-list [2.4Ghz|5Ghz]} {<CHANNEL-LIST>}

off-channel-scan {max-multicast <0-100>|scan-interval <2-100>}

off-channel-scan {sniffer-redirect tzsp <IP>}
```

Parameters

```
off-channel-scan {channel-list [2.4Ghz|5Ghz]} {<CHANNEL-LIST>}
```

off-channel-scan	Enables off channel scanning parameters. These parameters are optional, and the system configures default settings if no values are specified.
channel-list [2.4GHz|5GHz]	Optional. Specifies the channel list to scan • 2.4GHz – Selects the 2.4 GHz band • 5GHz – Selects the 5.0 GHz band
<CHANNEL-LIST>	Optional. Specifies a list of 20 MHz or 40 MHz channels for the selected band (the channels are separated by commas or hyphens)

```
off-channel-scan {max-multicast <0-100>|scan-interval <2-100>}
```

off-channel-scan	Enables off-channel scanning on this radio. These parameters are optional, and the system configures default settings if no values are specified.
max-multicast <0-100>	Optional. Configures the maximum multicast/broadcast messages to perform OCS • <0-100> – Specify a value from 0 - 100. The default is 4.
scan-interval <2-100>	Optional. Configures the scan interval in dtims • <2-100> – Specify a value from 2 - 100. The default is 10 dtims.

```
off-channel-scan {sniffer-redirect tzsp <IP>}
```

off-channel-scan	Enables off channel scanning parameters. These parameters are optional, and the system configures default settings if no values are specified.
sniffer-redirect tzsp <IP>	Optional. Captures and redirects packets to an IP address running a packet capture analysis tool • tzsp – Encapsulates captured packets in TZSP before redirecting • <IP> – Specify the destination device IP address.

Example

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#off-channel-scan
channel-list 2.4GHz 1

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  data-rates b-only
  mesh client
  off-channel-scan channel-list 2.4GHz 1
  guard-interval long
  aggregation ampdu tx-only
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  non-unicast tx-rate bss 1 dynamic-all
  non-unicast tx-rate bss 2 highest-basic
  non-unicast tx-rate bss 3 highest-basic
  non-unicast tx-rate bss 4 highest-basic
  non-unicast tx-rate bss 5 highest-basic
  non-unicast tx-rate bss 6 highest-basic
  non-unicast tx-rate bss 7 highest-basic
  non-unicast tx-rate bss 8 highest-basic
  non-unicast tx-rate bss 9 highest-basic
  non-unicast tx-rate bss 10 highest-basic
  non-unicast tx-rate bss 11 highest-basic
  non-unicast tx-rate bss 12 highest-basic
  non-unicast tx-rate bss 13 highest-basic
  non-unicast tx-rate bss 14 highest-basic
  non-unicast tx-rate bss 15 highest-basic
--More--
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands:

no	Disables radio off channel scanning

placement

interface-config-radio-instance

Defines the location where the radio is deployed. The radio's placement should depend on the country of operation selected and its regulatory domain requirements for radio emissions.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
placement [indoor|outdoor]
```

Parameters

```
placement [indoor|outdoor]
```

indoor	Radio is deployed indoors (uses indoor regulatory rules). This is the default setting.
outdoor	Radio is deployed outdoors (uses outdoor regulatory rules)

Example

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#placement outdoor

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  data-rates b-only
  placement outdoor
  mesh client
  off-channel-scan channel-list 2.4GHz 1
  guard-interval long
  aggregation ampdu tx-only
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  non-unicast tx-rate bss 1 dynamic-all
  non-unicast tx-rate bss 2 highest-basic
  non-unicast tx-rate bss 3 highest-basic
  non-unicast tx-rate bss 4 highest-basic
  non-unicast tx-rate bss 5 highest-basic
  non-unicast tx-rate bss 6 highest-basic
  non-unicast tx-rate bss 7 highest-basic
  non-unicast tx-rate bss 8 highest-basic
  non-unicast tx-rate bss 9 highest-basic
  non-unicast tx-rate bss 10 highest-basic
  non-unicast tx-rate bss 11 highest-basic
  non-unicast tx-rate bss 12 highest-basic
  non-unicast tx-rate bss 13 highest-basic
  non-unicast tx-rate bss 14 highest-basic
--More--
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands:

no	Resets a radio's deployment location

power

interface-config-radio-instance

Configures a radio's transmit power setting

The *transmit power control* (TPC) mechanism automatically reduces the used transmission output power when other networks are within range. Reduced power results in reduced interference issues and increased battery capacity.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
power [<1-30>|smart]
```

Parameters

```
power [<1-30>|smart]
```

power	Configures a radio's transmit power
<1-30>	Transmits power in dBm (actual power could be lower based on regulatory restrictions)
smart	Smart RF determines the optimum transmit power needed

Example

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#power 12

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  power 12
  data-rates b-only
  placement outdoor
  mesh client
  off-channel-scan channel-list 2.4GHz 1
  guard-interval long
  aggregation ampdu tx-only
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  non-unicast tx-rate bss 1 dynamic-all
  non-unicast tx-rate bss 2 highest-basic
  non-unicast tx-rate bss 3 highest-basic
  non-unicast tx-rate bss 4 highest-basic
  non-unicast tx-rate bss 5 highest-basic
  non-unicast tx-rate bss 6 highest-basic
  non-unicast tx-rate bss 7 highest-basic
  non-unicast tx-rate bss 8 highest-basic
  non-unicast tx-rate bss 9 highest-basic
  non-unicast tx-rate bss 10 highest-basic
  non-unicast tx-rate bss 11 highest-basic
  non-unicast tx-rate bss 12 highest-basic
  non-unicast tx-rate bss 13 highest-basic
--More--
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands:

no	Resets a radio's transmit power

preamble-short

interface-config-radio-instance

Enables short preamble on this radio. If using an 802.11bg radio, enable short preamble. Short preambles improve throughput. However, some devices (SpectraLink phones) require long preambles. This option is disabled by default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
preamble-short
```

Parameters

None

Example

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#preamble-short

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  power 12
  data-rates b-only
  placement outdoor
  mesh client
  off-channel-scan channel-list 2.4GHz 1
  preamble-short
  guard-interval long
  aggregation ampdu tx-only
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  non-unicast tx-rate bss 1 dynamic-all
  non-unicast tx-rate bss 2 highest-basic
  non-unicast tx-rate bss 3 highest-basic
  non-unicast tx-rate bss 4 highest-basic
  non-unicast tx-rate bss 5 highest-basic
  non-unicast tx-rate bss 6 highest-basic
  non-unicast tx-rate bss 7 highest-basic
  non-unicast tx-rate bss 8 highest-basic
  non-unicast tx-rate bss 9 highest-basic
  non-unicast tx-rate bss 10 highest-basic
  non-unicast tx-rate bss 11 highest-basic
  non-unicast tx-rate bss 12 highest-basic
--More--
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands:

no	Disables the use of short preamble on a radio

probe-response

interface-config-radio-instance

Configures transmission parameters for probe response frames

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
probe-response [rate|retry]
probe-response rate [follow-probe-request|highest-basic|lowest-basic]
```

Parameters

```
probe-response retry
```

probe-response	Configures transmission parameters for probe response frames
retry	Retransmits probe response if no acknowledgement is received from the client. This option is enabled by default.

```
probe-response rate [follow-probe-request|highest-basic|lowest-basic]
```

probe-response	Configures transmission parameters for probe response frames
rate	Configures data transmission rates used for the transmission of probe responses
follow-probe-request	Transmits probe responses at the same rate as the received request (default setting)
highest-basic	Uses the highest configured basic rate
lowest-basic	Uses the lowest configured basic rate

Example

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#probe-response rate
follow-probe-request
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands:

no	Resets transmission parameters for probe response frames

radio-resource-measurement

interface-config-radio-instance

Enables 802.11k radio resource measurement. When enabled, the radio station sends channel and neighbor reports.

The IEEE 802.11 Task Group k defined a set of specifications regarding radio resource measurements. These specifications specify the radio resources to be measured and the mechanism used to communicate measurement requests and results.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
radio-resource-measurement [attenuation-threshold <1-199>|max-entries <1-12>]
```

Parameters

```
radio-resource-measurement [attenuation-threshold <1-199>|max-entries <1-12>]
```

attenuation-threshold <1-199>	Configures the neighbor attenuation threshold, considered when generating channel and neighbor reports • <1-199> – Specify the attenuation threshold from 1 -199.
max-entries <1-12>	Configures the maximum number of entries to include in channel and neighbor reports • <1-12> – Specify a value from 1 - 12.

Example

```
rfs4000-229D58(config-device-00-23-68-22-9D-587-if-radio1)#radio-resource-mea
surement attenuation-threshold 20
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-587-if-radio1)#

rfs4000-229D58(config-device-00-23-68-22-9D-587-if-radio1)#radio-resource-mea
surement max-entries 10
rfs4000-229D58(config-device-00-23-68-22-9D-587-if-radio1)#

rfs4000-229D58(config-device-00-23-68-22-9D-587-if-radio1)#show context
 interface radio1
  radio-resource-measurement max-entries 10
  radio-resource-measurement attenuation-threshold 20
rfs4000-229D58(config-device-00-23-68-22-9D-587-if-radio1)#
```

Related Commands:

no	Disables 802.11k radio resource measurement support

radio-share-mode

interface-config-radio-instance

Configures a radio's mode of operation as Radio Share. A radio operating in the Radio Share mode services clients and also performs sensor functions (defined by the radio's *AirDefense Services Platform* (ADSP) licenses and profiles).

NOTE
The sensor capabilities of the radio are restricted to the channel and WLANs defined on the radio.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
radio-share-mode [inline|off|promiscuous]
```

Parameters

```
radio-share-mode [inline|off|promiscuous]
```

radio-share-mode	Configures the Radio Share mode of operation. The options are: inline, off, and promiscuous
inline	Enables sharing of all WLAN packets (matching the BSSID of the radio) serviced by the radio. In the inline mode, all packets are shared with the WIPS sensor module.
off	Disables Radio Share (no packets shared with WIPS sensor module)
promiscuous	Enables the sharing of packets received in the promiscuous mode (i.e. without filtering based on BSSI). In the promiscuous mode, the radio captures every frame it sees on the channel it is set for.

Example

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#radio-share-mode
promiscuous

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  power 12
  data-rates b-only
  placement outdoor
```

```
  mesh client
  off-channel-scan channel-list 2.4GHz 1
  preamble-short
  guard-interval long
  ....................................................
  non-unicast queue bss 16 50
  antenna-diversity
  max-clients 100
  radio-share-mode promiscuous
  airtime-fairness prefer-ht weight 6
  lock-rf-mode
  extended-range 15
  antenna-downtilt
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands:

no	Resets the radio share mode for this radio to its default

rate-selection

interface-config-radio-instance

Sets the rate selection method to standard or opportunistic

NOTE
This feature is not supported on RFS4011 wireless controller.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
rate-selection [opportunistic|standard]
```

Parameters

```
rate-selection [opportunistic|standard]
```

rate-selection	Sets the rate selection method to standard or opportunistic
standard	Configures the monotonic rate selection mode. This is the default setting.
opportunistic	Configures the opportunistic (ORLA) rate selection mode The ORLA algorithm is designed to select data rates that provide the best throughput. Instead of using local conditions to decide whether a data rate is acceptable or not, ORLA is designed to proactively probe other rates to determine if greater throughput is available. If these other rates do provide improved throughput, ORLA intelligently adjusts its selection tables to favour higher performance. ORLA provides improvements both on the client side of a mesh network as well as in the backhaul capabilities. ORLA is a key differentiator at the deployment and customer level and will be further explored in this paper.

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#rate-selection
opportunistic
%% Error: Rate selection cannot be changed for device [rfs4000]
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#
```

Related Commands:

no	Resets the rate selection mode to standard (monotonic)

remove-override

interface-config-radio-instance

Removes the radio's channel of operation

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
remove-override channel
```

Parameters

```
remove-override channel
```

remove-override channel	Removes the radio's channel of operation

Example

```
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-radio1)#show
context
 interface radio1
  channel 9
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-radio1)#

rfs4000-229D58(config-profile-testBrocade Mobility
RFS4000-if-radio1)#remove-override channel
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-radio1)#

rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-radio1)#show
context
 interface radio1
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-radio1)#
```

rf-mode

interface-config-radio-instance

Configures the radio's RF mode of operation

This command sets the mode to either 2.4 GHz WLAN or 5.0 GHz WLAN support depending on the radio's intended client support. If you are currently licensed to use 4.9 GHz, configure the 4.9 GHz-WLAN option.

Set the mode to sensor if using the radio for rogue device detection. The radio cannot support rogue detection when one of the other radios is functioning as a WIPS sensor. To set a radio as a detector, disable sensor support on the other access point radio.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
rf-mode [2.4GHz-wlan|4.9GHz-wlan|5GHz-wlan|client-bridge|scan-ahead|sensor]
```

Parameters

```
rf-mode [2.4GHz-wlan|4.9GHz-wlan|5GHz-wlan|client-bridge|scan-ahead|sensor]
```

rf-mode	Configures the radio's RF mode of operation
2.4GHz-wlan	Provides WLAN service in the 2.4 GHz bandwidth
4.9GHz-wlan	Provides WLAN service in the 4.9 GHz bandwidth
5GHz-wlan	Provides WLAN service in the 5.0 GHz bandwidth
client-bridge	Enables this radio to operate as a client bridge radio
scan-ahead	Enables this radio to operate as a scan-ahead radio A radio functioning in the scan-ahead mode is used for forward scanning only. The radio does not support WLAN or Mesh services. The scan ahead feature is used in *Dynamic Frequency Selection* (DFS) aware countries for infrastructure devices, static, and *vehicular mounted modems* (VMMs). It enables a secondary radio to scan ahead for an active channel for backhaul transmission, in the event of a radar trigger on the primary radio. The device then switches radios allowing transmission to continue. This is required in environments where handoff is required and DFS triggers are common. With a secondary radio dedicated for forward scanning, the primary radio, in case of radar hit, hands over the *channel availability check* (CAC) function to the secondary radio. This avoids a break in data communication, which would have resulted if the primary radio was to do CAC itself. The secondary radio periodically does a scan of the configured channel list, searching for the other available meshpoint roots. When configured on the root meshpoint, the scan-ahead feature also scans for cleaner channels.
sensor	Operates as a sensor radio. Configures this radio to function as a scanner, providing scanning services on both 2.4 GHz and 5.0 GHz bands. The radio does not provide WLAN services.

Example

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#rf-mode sensor

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  rf-mode sensor
  placement outdoor
  mesh client
  off-channel-scan channel-list 2.4GHz 1
  guard-interval long
  aggregation ampdu tx-only
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  non-unicast tx-rate bss 1 dynamic-all
  --More--
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands:

no	Resets the radio's RF mode of operation
data-rates	Configures the 802.11 data rates on this radio

rifs

interface-config-radio-instance

Configures *Reduced Interframe Spacing* (RIFS) parameters on this radio

This value determines whether interframe spacing is applied to access point transmitted or received packets, both, or none.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
rifs [none|rx-only|tx-only|tx-rx]
```

Parameters

```
rifs [none|rx-only|tx-only|tx-rx]
```

rifs	Configures RIFS parameters
none	Disables support for RIFS Consider setting the value to None for high-priority traffic to reduce packet delay.
rx-only	Supports RIFS possession only
tx-only	Supports RIFS transmission only
tx-rx	Supports both RIFS transmission and possession (default setting)

Example

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#rifs tx-only

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  rf-mode sensor
  placement outdoor
  mesh client
  off-channel-scan channel-list 2.4GHz 1
  guard-interval long
  aggregation ampdu tx-only
  rifs tx-only
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  non-unicast tx-rate bss 1 dynamic-all
  non-unicast tx-rate bss 2 highest-basic
  non-unicast tx-rate bss 3 highest-basic
  non-unicast tx-rate bss 4 highest-basic
  non-unicast tx-rate bss 5 highest-basic
  non-unicast tx-rate bss 6 highest-basic
  non-unicast tx-rate bss 7 highest-basic
  non-unicast tx-rate bss 8 highest-basic
```

```
  non-unicast tx-rate bss 9 highest-basic
  non-unicast tx-rate bss 10 highest-basic
  non-unicast tx-rate bss 11 highest-basic
  non-unicast tx-rate bss 12 highest-basic
  non-unicast tx-rate bss 13 highest-basic
--More--
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands:

no	Disables radio's RIFS parameters

rts-threshold

interface-config-radio-instance

Configures the *Request to Send* (RTS) threshold value on this radio

RTS is a transmitting station's signal that requests a *Clear To Send* (CTS) response from a receiving client. This RTS/CTS procedure clears the air where clients are contending for transmission time. Benefits include fewer data collisions and better communication with nodes that are hard to find (or hidden) because of other active nodes in the transmission path.

The RTS threshold controls RTS/CTS by initiating an RTS/CTS exchange for data frames larger than the threshold, and sends (without RTS/CTS) any data frames smaller than the threshold.

Consider the trade-offs when setting an appropriate RTS threshold for the WLAN's access point radios. A lower RTS threshold causes more frequent RTS/CTS exchanges. This consumes more bandwidth because of additional latency (RTS/CTS exchanges) before transmissions can commence. A disadvantage is the reduction in data-frame throughput. An advantage is quicker system recovery from electromagnetic interference and data collisions. Environments with more wireless traffic and contention for transmission make the best use of a lower RTS threshold.

A higher RTS threshold minimizes RTS/CTS exchanges, consuming less bandwidth for data transmissions. A disadvantage is less help to nodes that encounter interference and collisions. An advantage is faster data-frame throughput. Environments with less wireless traffic and contention for transmission make the best use of a higher RTS threshold.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
rts-threshold <0-65536>
```

Parameters

```
rts-threshold <0-65536>
```

<0-65536>	Specify the RTS threshold value from 0- 65536 bytes.

Example

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#rts-threshold 100

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
```

```
  rf-mode sensor
  placement outdoor
  mesh client
  rts-threshold 100
  off-channel-scan channel-list 2.4GHz 1
  guard-interval long
  aggregation ampdu tx-only
  rifs tx-only
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  non-unicast tx-rate bss 1 dynamic-all
  non-unicast tx-rate bss 2 highest-basic
  non-unicast tx-rate bss 3 highest-basic
  non-unicast tx-rate bss 4 highest-basic
  non-unicast tx-rate bss 5 highest-basic
 --More--
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands:

no	Resets a radio's RTS threshold to its default

shutdown

interface-config-radio-instance

Terminates or shuts down selected radio interface

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
shutdown
```

Parameters

None

Example

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)##shutdown
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands:

no	Enables a disabled radio interface

sniffer-redirect

interface-config-radio-instance

Captures and redirects packets to an IP address running a packet capture/analysis tool

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
sniffer-redirect [omnipeek|tzsp] <IP> channel [1|10|100|100w --------]
          {snap <1-65535> (append descriptor)}
```

Parameters

```
sniffer-redirect [omnipeek|tzsp] <IP> channel [1|10|100|100w ---------]
{snap <1-65535> (append descriptor)}
```

sniffer-redirect	Captures and redirects packets to an IP address running a packet capture/analysis tool
omnipeek	Encapsulates captured packets in proprietary header (use with OmniPeek and plug-in)
tzsp	Encapsulates captured packets in TZSP (used with WireShark and other tools)
<IP>	Specify the IP address of the device running the capture/analysis tool (the host to which captured off channel scan packets are redirected)
[1|10|100|100w ---------]	Specify the channel to capture packets • 1 – Channel 1 in 20 MHz mode (default setting) • 10 – Channel 10 in 20 MHz mode • 100 – Channel 100 in 20 MHz mode • 100w – Channels 100w in 40 MHz mode (channels 100*,104)
snap <1-65535>	Optional – Allows truncating of large captured frames at a specified length (in bytes). This option is useful when capturing traffic with large frames. Use this option when only headers are needed for analysis, since it reduces the bandwidth needed for sniffing, and (for typical values) eliminates any fragmentation of the outer packet. • <1-65535> – Specify the maximum truncated byte length of captured packets
append descriptor	Optional – Enables appending of the radio's receive descriptor to the captured packet

Example

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#sniffer-redirect
omnipeek 172.16.10.1 channel 1

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  rf-mode sensor
  placement outdoor
  mesh client
  rts-threshold 100
  off-channel-scan channel-list 2.4GHz 1
  guard-interval long
  aggregation ampdu tx-only
  rifs tx-only
  sniffer-redirect omnipeek 172.16.10.1 channel 1
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  non-unicast tx-rate bss 1 dynamic-all
  non-unicast tx-rate bss 2 highest-basic
  non-unicast tx-rate bss 3 highest-basic
  non-unicast tx-rate bss 4 highest-basic
  non-unicast tx-rate bss 5 highest-basic
  non-unicast tx-rate bss 6 highest-basic
 --More--
```

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands:

no	Disables packet capture and redirection

stbc

interface-config-radio-instance

Configures the radio's *Space Time Block Coding* (STBC) mode. STBC is a pre-transmission encoding scheme providing an improved SNR ratio (even at a single RF receiver). STBC transmits multiple data stream copies across multiple antennas. The receiver combines the copies into one to retrieve data from the signal. These transmitted data versions provide redundancy to increase the odds of receiving data streams with a good data decode (especially in noisy environments).

NOTE
STBC requires the radio has at least two antennas with the capability to transmit two streams. If the antenna mode is configured to 1x1 (or falls back to 1x1 for some reason), STBC support is automatically disabled.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
stbc [none|tx-only]
```

Parameters

```
stbc [none|tx-only]
```

none	Disables STBC support (default setting)
tx-only	Configures the AP radio to format and broadcast the special stream (enables STBC support for transmit only)

Example

```
rfs7000-37FABE(config-profile-81xxTestProfile-if-radio1)#stbc tx-only
rfs7000-37FABE(config-profile-81xxTestProfile-if-radio1)#

rfs7000-37FABE(config-profile-81xxTestProfile-if-radio1)#show context
 interface radio1
  stbc tx-only
rfs7000-37FABE(config-profile-81xxTestProfile-if-radio1)#
```

Related Commands:

no	Disables STBC support

use

interface-config-radio-instance

Enables an association ACL policy and a radio QoS policy for this radio interface

An association ACL is a policy-based *Access Control List* (ACL) that either prevents or allows wireless clients from connecting to a controller managed access point radio. An ACL is a sequential collection of permit and deny conditions that apply to controller packets. When a packet is received on an interface, the controller compares the fields in the packet against any applied ACLs to verify the packet has the required permissions to be forwarded, based on the criteria specified in the access lists. If a packet does not meet any of the criteria specified in the ACL, the packet is dropped.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
use [association-acl-policy|radio-qos-policy]

use [association-acl-policy <ASSOC-ACL-POLICY-NAME>|radio-qos-policy
<RADIO-QOS-
          POLICY-NAME>]
```

Parameters

```
use [association-acl-policy <ASSOC-ACL-POLICY-NAME>|radio-qos-policy
<RADIO-QOS-POLICY-NAME>]
```

association-acl-policy	Uses a specified association ACL policy with this radio interface • <ASSOC-ACL-POLICY-NAME> – Specify the association ACL policy name (should be existing and fully configured).
radio-qos-policy	Uses a specified radio QoS policy with this radio interface • <RADIO-QoS-POLICY-NAME> – Specify the radio QoS policy name (should be existing and fully configured).

Example

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#use
association-acl-policy test

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  rf-mode sensor
  placement outdoor
  mesh client
  rts-threshold 100
  off-channel-scan channel-list 2.4GHz 1
  guard-interval long
  aggregation ampdu tx-only
  rifs tx-only
  use association-acl-policy test
  sniffer-redirect omnipeek 172.16.10.1 channel 1
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  non-unicast tx-rate bss 1 dynamic-all
  non-unicast tx-rate bss 2 highest-basic
  non-unicast tx-rate bss 3 highest-basic
--More--
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands:

no	Dissociates the specified association ACL policy and radio QoS policy

wireless-client

interface-config-radio-instance

Configures wireless client parameters on this radio

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
wireless-client tx-power [<0-20>|mode]

wireless-client tx-power mode [802.11d {symbol-ie}|symbol-ie {802.11d}]
```

Parameters

```
wireless-client tx-power <0-20>
```

wireless-client	Configures wireless client parameters
tx-power <0-20>	Configures the transmit power indicated to wireless clients • <0-20> – Specify transmit power from 0 - 20 dBm

```
wireless-client tx-power mode [802.11d {symbol-ie}|symbol-ie {802.11d}]
```

wireless-client	Configures wireless client parameters
tx-power [802.11d|symbol-ie]	Configures the transmit power indicated to wireless clients • 802.11d – Advertises in the IEEE 802.11d country information element • symbol-ie – Optional. • symbol-ie – Advertises in the Symbol (176) • 802.11d – Optional. Advertises in the IEEE 802.11d country information element

Example

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#wireless-client
tx-power 20

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  rf-mode sensor
  placement outdoor
  mesh client
  rts-threshold 100
  wireless-client tx-power 20
  off-channel-scan channel-list 2.4GHz 1
  guard-interval long
  aggregation ampdu tx-only
  rifs tx-only
  use association-acl-policy test
  sniffer-redirect omnipeek 172.16.10.1 channel 1
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  non-unicast tx-rate bss 1 dynamic-all
```

```
 --More--
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands:

no	Resets the transmit power indicated to wireless clients

wlan

interface-config-radio-instance

Enables a WLAN on this radio

Use this command to configure WLAN/BSS mappings for an existing access point deployment. Administrators can assign each WLAN its own BSSID. If using a single-radio access point, there are 8 BSSIDs available. If using a dual-radio access point there are 8 BSSIDs for the 802.11b/g/n radio and 8 BSSIDs for the 802.11a/n radio.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
wlan <WLAN-NAME> {bss|primary}

wlan <WLAN-NAME> {bss <1-8> {primary}}
```

Parameters

```
wlan <WLAN-NAME> {bss <1-8> {primary}}
```

<WLAN-NAME> {bss <1-8> |primary}	Specify the WLAN name (it must have been already created and configured) • bss <1-8> – Optional. Specifies a BSS for the radio to map the WLAN • <1-8> – Specify the BSS number from 1 - 8. • primary – Optional. Uses the specified WLAN as the primary WLAN, when multiple WLANs exist on the BSS • primary – Optional. Uses the specified WLAN as the primary WLAN, when multiple WLANs exist on the BSS

Example

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#wlan TestWLAN
primary

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  rf-mode sensor
  placement outdoor
  mesh client
  rts-threshold 100
  wireless-client tx-power 20
  wlan TestWLAN bss 1 primary
  off-channel-scan channel-list 2.4GHz 1
  guard-interval long
  aggregation ampdu tx-only
  rifs tx-only
  use association-acl-policy test
```

```
  sniffer-redirect omnipeek 172.16.10.1 channel 1
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  non-unicast tx-rate bss 1 dynamic-all
  non-unicast tx-rate bss 2 highest-basic
  non-unicast tx-rate bss 3 highest-basic
  non-unicast tx-rate bss 4 highest-basic
  non-unicast tx-rate bss 5 highest-basic
  non-unicast tx-rate bss 6 highest-basic
  --More--
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands:

no	Disables a WLAN on a radio

interface-config-wwan-instance

interface

A *Wireless Wide Area Network* (WWAN) card is a specialized network interface card that allows a network device to connect, transmit and receive data over a cellular WAN. Brocade Mobility 7131 Access Point model access points, Brocade Mobility RFS4000 and Brocade Mobility RFS6000 controllers utilize a PCI express card slot that supports 3G WWAN cards. The WWAN card uses *point-to-point protocol* (PPP) to connect to the *Internet Service Provider* (ISP) and gain access to the Internet. PPP establishes internet links over dial-up modems, DSL connections, and many other types of point-to-point communications. PPP packages your system's TCP/IP packets and forwards them to the serial device where they can be put on the network. PPP is a full-duplex protocol used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of *High Speed Data Link Control* (HDLC) for packet encapsulation.

To switch to the WWAN Interface configuration mode, use the following command:

```
<DEVICE>(config)#profile <DEVICE-TYPE> <DEVICE-PROFILE-NAME>

rfs4000-229D58(config)#profile rfs4000 testBrocade Mobility RFS4000
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000)#

<DEVICE>(config-profile-<DEVICE-PROFILE-NAME>)#interface wwan1

rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-wwan1)#?
Interface configuration commands:
  apn          Enter the access point name provided by the service provider
  auth-type    Type of authentication, Eg chap, pap
  crypto       Encryption Module
  description  Port description
  ip           Internet Protocol (IP)
  no           Negate a command or set its defaults
  password     Enter password provided by the service provider
  shutdown     Disable wireless wan feature
  use          Set setting to use
  username     Enter username provided by the service provider

  clrscr       Clears the display screen
  commit       Commit all changes made in this session
  do           Run commands from Exec mode
  end          End current mode and change to EXEC mode
```

```
  exit          End current mode and down to previous mode
  help          Description of the interactive help system
  revert        Revert changes
  service       Service Commands
  show          Show running system information
  write         Write running configuration to memory or terminal

rfs4000-229D58(config-profile-<PROFILE-NAME>-if-wwan1)#
```

NOTE
The WWAN interface is supported only on the Brocade Mobility 7131 Access Point, Brocade Mobility RFS4000, Brocade Mobility RFS6000 platforms.

The following table summarizes WWAN interface configuration commands.

Commands	Description	Reference
apn	Configures the access point's name provided by the service provider	page 734
auth-type	Configures the authentication types used on this interface	page 735
crypto	Associates a crypto map with this interface	page 735
description	Configures a unique description for this interface	page 736
ip	Associates an IP ACL with this interface	page 737
no	Removes or reverts the WWAN interface settings	page 738
password	Configures a password for this WWAN interface	page 738
use	Associates an IP ACL with this interface	page 739
username	Configures the names of users accessing this interface	page 740

apn

interface-config-wwan-instance

Configures the access point's name provided by the service provider. This setting is needed in areas with multiple cellular data providers using the same protocols, such as Europe and Asia.

Supported in the following platforms:

- Access Points — Brocade Mobility 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000

Syntax:

```
apn <WORD>
```

Parameters

```
apn <WORD>
```

apn <WORD>	Specify the service provided given access point name.

Example

```
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-wwan1)#apn
TechPubs
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-wwan1)#
```

```
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-wwan1)#show
context
 interface wwan1
  apn TechPubs
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-wwan1)#
```

Related Commands:

no	Removes the configured access point name.

auth-type

interface-config-wwan-instance

Configures the authentication types used on this interface

Supported in the following platforms:

- Access Points — Brocade Mobility 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000

Syntax:

```
auth-type [chap|mschap|mschap-v2|pap]
```

Parameters

```
auth-type [chap|mschap|mschap-v2|pap]
```

auth-type	Configures the authentication protocol used on this interface
chap	Configures *Challenge-Handshake Authentication Protocol* (CHAP). This is the default value.
mschap	Configures *Microsoft Challenge-Handshake Authentication Protocol* (MSCHAP)
mschapv2	Configures *Microsoft Challenge-Handshake Authentication Protocol* (MSCHAP) version 2
pap	Configures *Password Authentication Protocol* (PAP)

Example

```
rfs4000-229D58(config-profile-testBrocade Mobility
RFS4000-if-wwan1)#auth-type mschap-v2
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-wwan1)#

rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-wwan1)#show
context
 interface wwan1
  apn TechPubs
  auth-type mschap-v2
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-wwan1)#
```

Related Commands:

no	Removes the authentication protocol configured on this interface

crypto

interface-config-wwan-instance

Associates a crypto map with this interface

Supported in the following platforms:

- Access Points — Brocade Mobility 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000

Syntax:

```
crypto map <CRYPTO-MAP-NAME>
```

Parameters

```
crypto map <CRYPTO-MAP-NAME>
```

crypto map <CRYPTO-MAP-NAME>	Associates a crypto map with this interface • <CRYPTO-MAP-NAME> – Specify the crypto map name (should be existing and configured)

Example

```
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-wwan1)#crypto
map test
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-wwan1)#

rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-wwan1)#show
context
 interface wwan1
  apn TechPubs
  auth-type mschap-v2
  crypto map test
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-wwan1)#
```

Related Commands:

no	Removes the crypto map associated with this interface

description

interface-config-wwan-instance

Configures a unique description for this interface

Supported in the following platforms:

- Access Points — Brocade Mobility 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000

Syntax:

```
description <WORD>
```

Parameters

```
description <WORD>
```

description <WORD>	Configures a unique description for this WWAN interface

Example

```
ap7131-11E6C4(config-device-00-23-68-11-E6-C4-if-wwan1)#description "This
interf
ace is reserved for the the ISP Airtel"
% Error: Unknown config-item (id:description)
```

```
ap7131-11E6C4(config-device-00-23-68-11-E6-C4-if-wwan1)#

rfs4000-229D58(config-profile-testRFS4000-if-wwan1)#description "This
interface
is reserved for the ISP Airtel"
% Error: Unknown config-item (id:description)
rfs4000-229D58(config-profile-testRFS4000-if-wwan1)#
```

Related Commands:

no	Removes the description configured for this WWAN interface

ip

interface-config-wwan-instance

Configures IP related settings on this interface

Supported in the following platforms:

- Access Points — Brocade Mobility 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000

Syntax:

```
ip [default-gateway|nat]

ip default-gateway priority <1-8000>

ip nat [inside|outside]
```

Parameters

```
ip default-gateway priority <1-8000>
```

ip	Configures IP related settings on this interface
default-gateway priority <1-8000>	Configures the default-gateway's (learned by the wireless WAN) priority. • <1-8000> – Specify a value from 1 - 8000. The default is 3000.

```
ip nat [inside|outside]
```

ip	Configures IP related settings on this interface
nat [inside|outside]	Configures the NAT settings • inside – Marks this WWAN interface as NAT inside • outside – Marks this WWAN interface as NAT outside

Example

```
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-wwan1)#ip
default-gateway priority 1
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-wwan1)#

rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-wwan1)#ip nat
inside
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-wwan1)#

rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-wwan1)#show
context
 interface wwan1
```

```
  apn TechPubs
  auth-type mschap-v2
  crypto map test
  ip nat inside
  ip default-gateway priority 1
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-wwan1)#
```

Related Commands:

no	Removes IP related settings on this interface

no

interface-config-wwan-instance

Removes or reverts the WWAN interface settings

Supported in the following platforms:

- Access Points — Brocade Mobility 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000

Syntax:

```
no [all|apn|auth-type|crypto|description|ip|password|shutdown|use|username]
```

Parameters

None

Usage Guidelines:

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-wwan1)#no apn

rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-wwan1)#no
auth-type
```

Related Commands:

apn	Configures the access point's name provided by the service provider
auth-type	Configures the authentication types used on this interface
crypto	Associates a crypto map with this interface
description	Configures a unique description for this interface
ip	Configures IP related settings on this interface
password	Configures a password for this WWAN interface
use	Associates an IP ACL with this interface
username	Configures the names of users accessing this interface

password

interface-config-wwan-instance

Configures a password for this WWAN interface. The configured value is used for authentication support by the cellular data carrier.

Supported in the following platforms:

- Access Points — Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000

Syntax:

```
password [2 <WORD>|<WORD>]
```

Parameters

```
password [2 <WORD>|<WORD>]
```

2 <WORD>	Configures an encrypted password. Use this option when copy pasting the password from another device.
<WORD>	Enter the password string (should not exceed 32 characters in length.

Example

```
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-wwan1)#password
TechPubsTesting@123
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-wwan1)#

rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-wwan1)#show
context
 interface wwan1
  password TechPubsTesting@123
  crypto map test
  ip nat inside
  ip default-gateway priority 1
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-wwan1)#
```

Related Commands:

no	Removes the configured password

use

interface-config-wwan-instance

Associates an IP ACL with this interface. The ACL should be existing and configured.

The ACL applies an IP based firewall to all incoming packets. The ACL identifies a single IP or a range of IPs that are to be allowed or denied access on this interface.

Supported in the following platforms:

- Access Points — Brocade Mobility 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000

Syntax:

```
use ip-access-list in <ACCESS-LIST-NAME>
```

Parameters

```
use ip-access-list in <ACCESS-LIST-NAME>
```

use ip-access-list in <ACCESS-LIST-NAME>	Associates an IP ACL with this interface • <ACCESS-LIST-NAME> – Specify the IP ACL name.

Example

```
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-wwan1)#use
ip-access-list in test
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-wwan1)#

rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-wwan1)#show
context
 interface wwan1
  password TechPubsTesting123
  crypto map test
  ip nat inside
  use ip-access-list in test
  ip default-gateway priority 1
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-wwan1)#
```

Related Commands:

no	Removes the IP ACL associated with this interface

username

interface-config-wwan-instance

Configures the names of users accessing this interface

Supported in the following platforms:

- Access Points — Brocade Mobility 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000

Syntax:

```
username <WORD>
```

Parameters

```
username <WORD>
```

username <WORD>	Configures the username for authentication support by the cellular data carrier • <WORD> – Specify the username (should not exceed 32 characters).

Example

```
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-wwan1)#username
TechPubsUser1

rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-wwan1)#show
context
 interface wwan1
  username TechPubsUser1
  password TechPubsTesting123
  crypto map test
  ip nat inside
  use ip-access-list in test
  ip default-gateway priority 1
```

```
rfs4000-229D58(config-profile-testBrocade Mobility RFS4000-if-wwan1)#
```

Related Commands:

no	Removes the configured username

interface-config-serial-instance

interface

This section describes the serial interface configuration commands.

Use the (config-profile-<DEVICE-PROFILE-NAME>) instance to configure the serial interface associated with the service platform.

To switch to this mode, use the following command:

```
<DEVICE>(config-profile-<DEVICE-PROFILE-NAME>)#interface ?

The following example uses the config-profile-default-nx4500 instance to
configure a serial interface:

nx4500-5CFA2B(config-profile-default-nx45xx)#interface ?
  WORD          Interface name
  fe            Select a FastEthernet interface
  ge            Select a GigabitEthernet interface
  me1           Select the management interface
  port-channel  Select a port channel interface
  pppoe1        Select the PPP Over Ethernet interface
  radio         Select a radioss
  serial        Select a serial interface (virtual interface)
  t1e1          Select a T1 or E1 interface
  up            Select the Uplink GigabitEthernet interface
  vlan          Select a vlan interface (switched virtual interface)
  vmif          Select the virtual interface
  wwan1         Select the wireless wan interface
  xge           Select a TenGigabitEthernet interface

nx4500-5CFA2B(config-profile-default-nx45xx)#interface

nx4500-5CFA2B(config-profile-default-nx45xx)#interface |serial-<1-4>/1:1|

nx4500-5CFA2B(config-profile-default-nx45xx)#interface serial-1/1:1
nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#

nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#?
Interface configuration commands:
  authentication            Type of authentication, Eg chap, pap
  description               Enter description provided by the service provider
  encapsulation             The type of traffic that this group handles.
  ip                        Internet Protocol (IP)
```

local-ip-address IP address assigned to the local system

no Negate a command or set its defaults

```
  password                  Enter password provided by the service provider
  remote-ip-subnet          IP subnet assigned to the remote system along with
                            subnet in CIDR notation
  remove-override           Remove override from the device
  shutdown                  Disable serial interface
```

```
use                         Set setting to use
username                    Enter username provided by the service provider

clrscr                      Clears the display screen
commit                      Commit all changes made in this session
do                          Run commands from Exec mode
end                         End current mode and change to EXEC mode
exit                        End current mode and down to previous mode
help                        Description of the interactive help system
revert                      Revert changes
service                     Service Commands
show                        Show running system information
write                       Write running configuration to memory or terminal

nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#
```

shutdown

interface-config-serial-instance

Shuts down the serial interface. Use the no shutdown command to re-start a serial interface.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
shutdown
```

Parameters

None

Example

```
nx4500-5CFA2B(config-profile-default-nx6500-if-serial-1/1:1)#shutdown
```

Related Commands:

no	Disables or reverts serial interface settings to their default

interface-config-t1e1-instance

interface

The T1/E1 interfaces are physical layer interfaces that support data, voice, or a combination of data and voice applications.

Use the (config-profile-<DEVICE-PROFILE-NAME>) instance to configure the T1E1 interface associated with the service platform.

To switch to this mode, use the following command:

<DEVICE>(config)#profile <DEVICE-TYPE> <DEVICE-PROFILE-NAME>

```
<DEVICE>(config-profile-<DEVICE-PROFILE-NAME>)#interface ?
```

Tinterface-config-vm-instance

interface

Mobility provides a dataplane bridge for external network connectivity for *Virtual Machines* (VMs). VM interfaces are layer 2 interfaces on Mobility bridge that define which IP address is associated with each VLAN ID the service platform is connected to and enables remote service platform administration. Each custom VM can have up to a maximum of two physical VM interfaces. Each VM interface can be mapped to one of sixteen VMIF ports on the dataplane bridge. This mapping determines the destination for service platform routing.

By default, VM interfaces are internally connected to the dataplane bridge via VMIF1. VMIF1 is an untagged port providing access to VLAN 1 to support the capability to connect the VM interfaces to any of the VMIF ports. This provides the flexibility to move a VM interface onto different VLANs as well as configure specific firewall and QOS rules.

Use the (config-profile-<DEVICE-PROFILE-NAME>) instance to configure the VM interface associated with the service platform profile.

To switch to this mode, use the following commands:

```
<DEVICE>(config)#profile <DEVICE-TYPE> <DEVICE-PROFILE-NAME>

<DEVICE>(config-profile-<DEVICE-PROFILE-NAME>)#interface ?
```

The following example uses the config-profile-default-nx45xx instance to configure a VM interface:

```
nx4500-5CFA2B(config-profile-default-nx45xx)#interface vmif ?
  <1-8>  Interface index

nx4500-5CFA2B(config-profile-default-nx45xx)#i

nx4500-5CFA2B(config-profile-default-nx45xx)#interface vmif 2
nx4500-5CFA2B(config-profile-default-nx45xx-if-vmif2)#

nx4500-5CFA2B(config-profile-default-nx45xx-if-vmif2)#?
VM Interface Mode commands:
  description  Port description
  ip           Internet Protocol (IP)
  no           Negate a command or set its defaults
  qos          Quality of service
  switchport   Set switching mode characteristics
  use          Set setting to use

  clrscr       Clears the display screen
  commit       Commit all changes made in this session
  do           Run commands from Exec mode
  end          End current mode and change to EXEC mode
  exit         End current mode and down to previous mode
  help         Description of the interactive help system
  revert       Revert changes
  service      Service Commands
  show         Show running system information
  write        Write running configuration to memory or terminal

nx4500-5CFA2B(config-profile-default-nx45xx-if-vmif2)#
```

```
nx9500-6C8809(config-profile-default-nx9000)#interface vmif ?
  <1-12>  Interface index

nx9500-6C8809(config-profile-default-nx9000)#

nx9500-6C8809(config-profile-default-nx9000)#interface vmif 2
nx9500-6C8809(config-profile-default-nx9000-if-vmif2)#?
VM Interface Mode commands:
  description  Port description
  ip           Internet Protocol (IP)
  no           Negate a command or set its defaults
  qos          Quality of service
  switchport   Set switching mode characteristics
  use          Set setting to use

  commit       Commit all changes made in this session
  end          End current mode and change to EXEC mode
  exit         End current mode and down to previous mode
  revert       Revert changes
  write        Write running configuration to memory or terminal

nx9500-6C8809(config-profile-default-nx9000-if-vmif2)#
```

The following table summarizes VM interface configuration commands.

Commands	Description	Reference
ip	Configures settings related to ARP and DHCP responses	page 744
no	Removes or reverts the VM interface settings	page 778

ip

Profile Config Commands

The following table summarizes NAT pool configuration commands.

Command	Description	Reference
ip	Configures IP components, such as default gateway, DHCP, DNS server forwarding, name server, domain name, routing standards etc.	page 744
nat-pool-config-instance	Invokes NAT pool configuration parameters	page 749

ip

ip

Configures IP components, such as default gateway, DHCP, DNS server forwarding, name server, domain name, routing standards etc.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
ip
[default-gateway|dhcp|dns-server-forward|domain-lookup|domain-name|igmp|name-
server|
          nat|route|routing]

ip default-gateway [<IP>|failover|priority [dhcp-client <1-1800>|static-route
<1-1800>]

ip [dns-server-forward|domain-lookup|domain-name <DOMAIN-NAME>|name-server
<IP>|
          routing]

ip dhcp client [hostname|persistent-lease]

ip igmp snooping {forward-unknown-multicast|querier}
ip igmp snooping {forward-unknown-multicast}
ip igmp snooping {querier} {max-response-time <1-25>|query-interval <1-18000>|
          robustness-variable <1-7>|timer expiry <60-300>|version <1-3>}
```

NOTE
The command 'ip igmp snooping' can be configured under bridge VLAN context also. For example:
`rfs7000-37FABE(config-device 00-15-70-37-FA-BE-bridge-vlan-1)#ip igmp snooping forward-unknown-multicast`

```
ip nat [crypto|inside|outside|pool]

ip nat [crypto source pool|pool] <NAT-POOL-NAME>

ip nat [inside|outside] [destination|source]

ip nat [inside|outside] destination static <ACTUAL-IP> <1-65535> [tcp|udp]
          [(<NATTED-IP> {<1-65535>})]

ip nat [inside|outside] source [list|static]

ip nat [inside|outside] source static <ACTUAL-IP> <1-65535> [tcp|udp]
          [(<NATTED-IP> {<1-65535>})]


ip nat [inside|outside] source list <IP-ACCESS-LIST-NAME> interface
[<INTERFACE-NAME>|
          pppoe1|vlan <1-4094>|wwan1] [(address <IP>|interface
<L3-IF-NAME>|overload|
          pool <NAT-POOL-NAME>)]

ip route <IP/M> <IP>
```

Parameters

	`ip default-gateway [<IP>|failover|priority [dhcp-client <1-1800>| static-route <1-1800>]`
default-gateway	Configures default gateway (next-hop router) parameters
<IP>	Configures default gateway's IP address • <IP> – Specify the default gateway's IP address.
failover	Configures failover to the gateway (with next higher priority) when the current default gateway is unreachable (In case of multiple default gateways)
priority [dhcp-client <1-1800>| static-route <1-1800>]	Configures default gateway priority • dhcp-client <1-1800> – Defines a priority for the default gateway acquired by the DHCP client– on the VLAN interface • static-route <1-1800> – Defines a priority for the statically configured default gateway The following keyword is common to 'dhcp-client' and 'static-route' parameters: • <1-1800> – Specify the priority from 1 - 18000 (lower the value higher is the priority).
	`ip [dns-server-forward|domain-lookup|domain-name <DOMAIN-NAME>|name-server <IP>| routing]`
dns-server-forward	Enables DNS forwarding. This command enables the forwarding of DNS queries to DNS servers outside of the network.
domain-lookup	Enables domain lookup
domain-name <DOMAIN-NAME>	Configures a default domain name • <DOMAIN-NAME> – Specify a name for the DNS.
name-server <IP>	Configures the name server's IP address • <IP> – Specify the IP address of the name server.
routing	Enables IP routing of logically addressed packets from their source to their destination
	`ip dhcp client [hostname|persistent-lease]`
dhcp	Configures the DHCP client and host
client [hostname|persistent-lease]	Sets the DHCP client • hostname – Includes the hostname in the DHCP request • persistent-lease – Retains the last lease across reboot if the DHCP server is unreachable
	`ip igmp snooping *{forward-unknown-multicast}*`
igmp snooping forward-unknown-multicast	Optional. Enables/disables unknown multicast data packets to be flooded in the specified VLAN. By default this feature is disabled.
	`ip igmp snooping *{querier} {max-response-time <1-25>|query-interval <1-18000>| robustness-variable <1-7>|timer expiry <60-300>|version <1-3>}*`
igmp snooping querier	Optional. Enables/disables the IGMP querier functionality for the specified VLAN. By default IGMP snooping querier is disabled.
max-response-time <1-25>	Configures the IGMP maximum query response interval used in IGMP V2/V3 queries for the given VLAN. The default is 10 seconds.
query-interval <1-18000>	Configures the IGMP querier query interval in seconds. Specify a value from 1 - 18000 seconds.
robustness-variable <1-7>	Configures the IGMP robustness variable from 1 - 7
timer expiry <60-300>	Configures the other querier time out value for the given VLAN. The default is 60 seconds.
version <1-3>	Configures the IGMP query version for the given VLAN. The default is 3.

```
ip nat [crypto source pool|pool <NAT-POOL-NAME>]
```

nat	Configures the NAT parameters
crypto source pool <NAT-POOL-NAME>	Configures the NAT source address translation settings for IPSec tunnels • <NAT-POOL-NAME> – Specify a NAT pool name.
pool <NAT-POOL-NAME>	Configures a pool of IP addresses for NAT • <NAT-POOL-NAME> – Specify a name for the NAT pool.

```
ip nat [inside|outside] destination static <ACTUAL-IP> <1-65535> [tcp|udp]
[(<NATTED-IP> {<1-65535>})]
```

nat	Configures the NAT parameters
[inside|outside]	Configures inside and outside address translation for the destination • inside – Configures inside address translation • outside – Configures outside address translation
destination static <ACTUAL-IP>	The following keywords are common to the 'inside' and 'outside' parameters: • destination – Specifies destination address translation parameters • static – Specifies static NAT local to global mapping • <ACTUAL-IP> – Specify the actual outside IP address to map.
<1-65535> [tcp|udp]	• <1-65535> – Configures the actual outside port. Specify a value from 1 - 65535. • tcp – Configures *Transmission Control Protocol* (TCP) port • udp – Configures *User Datagram Protocol* (UDP) port
<NATTED-IP> <1-65535>	Enables configuration of the outside natted IP address • <NATTED-IP> – Specify the outside natted IP address. • <1-65535> – Optional. Configures the outside natted port. Specify a value from 1 - 65535.

```
ip nat [inside|outside] source static <ACTUAL-IP> <1-65535> [tcp|udp]
[(<NATTED-IP> {<1-65535>})]
```

nat	Configures the NAT parameters
[inside|outside]	Configures inside and outside address translation for the source • inside – Configures inside address translation • outside – Configures outside address translation
source static <ACTUAL-IP>	The following keywords are common to the' inside' and 'outside' parameters: • source – Specifies source address translation parameters • static – Specifies static NAT local to global mapping • <ACTUAL-IP> – Specify the actual inside IP address to map.
<1-65535> [tcp|udp]	• <1-65535> – Configures the actual outside port. Specify a value from 1 - 65535. • tcp – Configures *Transmission Control Protocol* (TCP) port • udp – Configures *User Datagram Protocol* (UDP) port
<NATTED-IP> <1-65535>	Enables configuration of the outside natted IP address • <NATTED-IP> – Specify the outside natted IP address. • <1-65535> – Optional. Configures the outside natted port. Specify a value from 1 - 65535.

```
ip nat [inside|outside] source list <IP-ACCESS-LIST-NAME> interface
[<INTERFACE-NAME>|pppoe1|vlan <1-4094>|wwan1] [(address <IP>|interface
<L3-IF-NAME>|overload|
pool <NAT-POOL-NAME>)]
```

nat	Configures the NAT parameters
[inside|outside]	Configures inside and outside IP access list

source list <IP-ACCESS-LIST-NAME>	Configures an access list describing local addresses • <IP-ACCESS-LIST-NAME> – Specify a name for the IP access list.
interface [<INTERFACE-NAME>| pppoe1| vlan <1-4094>| wwan1]	Selects an interface to configure. Select a layer 3 router interface or a VLAN interface. • <INTERFACE-NAME> – Selects a layer 3 interface. Specify the layer 3 router interface name. • vlan – Selects a VLAN interface • <1-4094> – Set the SVI VLAN ID of the interface. • pppoe1 – Selects PPP over Ethernet interface • wwan1 – Selects Wireless WAN interface
address <IP>	The following keyword is recursive and common to all interface types: • address <IP> – Configures the interface IP address used with NAT
interface <L3-IF-NAME>	The following keyword is recursive and common to all interface types: • interface <L3-IF-NAME> – Configures a wireless controller or service platform's VLAN interface • <L3IFNAME> – Specify the SVI VLAN ID of the interface.
overload	The following keyword is recursive and common to all interface types: • overload – Enables use of global address for many local addresses
pool <NAT-POOL-NAME>	The following keyword is recursive and common to all interface types: • pool <NAT-POOL-NAME> – Specifies the NAT pool • <NAT-POOL-NAME> – Specify the NAT pool name.

```
ip route <IP/M> <IP>
```

route	Configures the static routes
<IP/M>	Specify the IP destination prefix in the A.B.C.D/M format.
<IP>	Specify the IP address of the gateway.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#ip default-gateway 172.16.10.4
rfs7000-37FABE(config-profile-default-rfs7000)#ip dns-server-forward
rfs7000-37FABE(config-profile-default-rfs7000)#ip nat inside source list test
interface vlan 1 pool pool1 overload

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
 ip default-gateway 172.16.10.4
 autoinstall configuration
 autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 interface me1
 interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
```

```
 interface ge2
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge3
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge4
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface pppoe1
 use firewall-policy default
 ip dns-server-forward
 ip nat inside source list test interface vlan1 pool pool1 overload
service pm sys-restart
 router ospf
rfs7000-37FABE(config-profile-default-rfs7000)#

rfs7000-37FABE(config-profile-default-rfs7000-nat-pool-pool1)#?
Nat Policy Mode commands:
  address  Specify addresses for the nat pool
  no       Negate a command or set its defaults

  clrscr   Clears the display screen
  commit   Commit all changes made in this session
  do       Run commands from Exec mode
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  revert   Revert changes
  service  Service Commands
  show     Show running system information
  write    Write running configuration to memory or terminal

rfs7000-37FABE(config-profile-default-rfs7000-nat-pool-pool1)
```

Related Commands:

no	Disables or reverts settings to their default

nat-pool-config-instance

ip

Use the config-profile-<DEVICE-PROFILE-NAME> instance to configure *Network Address Translation* (NAT) pool settings.

```
<DEVICE>(config-profile-default-<PROFILE-NAME>)#ip nat pool pool1
```

The following example uses the config-profile-default-rfs7000 instance to configure NAT pool settings:

```
<DEVICE>(config-profile-default-<PROFILE-NAME>)#ip nat pool pool1

rfs7000-37FABE(config-profile-default-rfs7000)#ip nat pool pool1
rfs7000-37FABE(config-profile-default-rfs7000-nat-pool-pool1)#ip nat pool
pool1
```

```
rfs7000-37FABE(config-profile-default-rfs7000-nat-pool-pool1)#?
Nat Policy Mode commands:
  address  Specify addresses for the nat pool
  no       Negate a command or set its defaults

  clrscr   Clears the display screen
  commit   Commit all changes made in this session
  do       Run commands from Exec mode
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  revert   Revert changes
  service  Service Commands
  show     Show running system information
  write    Write running configuration to memory or terminal

rfs7000-37FABE(config-profile-default-rfs7000-nat-pool-pool1)
```

The following table summarizes NAT pool configuration commands.

Command	Description	Reference
address	Configures NAT pool addresses	*page 7-750*
no	Negates a command or sets its default	*page 7-751*
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug (config-if) instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

address

nat-pool-config-instance

Configures NAT pool of IP addresses

Define a range of IP addresses hidden from the public Internet. NAT modifies network address information in the defined IP range while in transit across a traffic routing device. NAT only provides IP address translation and does not provide a firewall. A branch deployment with NAT by itself will not block traffic from being potentially routed through a NAT device. Consequently, NAT should be deployed with a stateful firewall.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
address [<IP>|range]
address range <START-IP> <END-IP>
```

Parameters

```
address [<IP>|range <START-IP> <END-IP>]
```

address <IP>	Adds a single IP address to the NAT pool
range <START-IP> <END-IP>	Adds a range of IP addresses to the NAT pool • <START-IP> – Specify the starting IP address of the range. • <END-IP> – Specify the ending IP address of the range.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-nat-pool-pool1)#address range
172.
16.10.2 172.16.10.8

rfs7000-37FABE(config-profile-default-rfs7000-nat-pool-pool1)#show context
 ip nat pool pool1
  address range 172.16.10.2 172.16.10.8
rfs7000-37FABE(config-profile-default-rfs7000-nat-pool-pool1)#
```

Related Commands:

no	Removes address(es) configured with this NAT pool

no

nat-pool-config-instance

Removes address(es) configured with this NAT pool

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no address
```

Parameters

None

Usage Guidelines:

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-nat-pool-pool1)#show context
 ip nat pool pool1
  address range 172.16.10.2 172.16.10.8
rfs7000-37FABE(config-profile-default-rfs7000-nat-pool-pool1)#

rfs7000-37FABE(config-profile-default-rfs7000-nat-pool-pool1)#no address
range 1
72.16.10.2 172.16.10.8

rfs7000-37FABE(config-profile-default-rfs7000-nat-pool-pool1)#show context
 ip nat pool pool1
rfs7000-37FABE(config-profile-default-rfs7000-nat-pool-pool1)#
```

Related Commands:

address	Configures NAT pool IP address(es)

l2tpv3

Profile Config Commands

Defines the L2TPV3 settings for tunneling layer 2 payloads using VPNs

L2TPv3 is an IETF standard that defines the control and encapsulation protocol settings for tunneling layer 2 frames in an IP network (and access point profile) between two IP nodes. Use L2TPv3 to create tunnels for transporting layer 2 frames. L2TPv3 enables Mobility supported controllers and access points to create tunnels for transporting Ethernet frames to and from bridge VLANs and physical ports. L2TPv3 tunnels can be defined between Mobility devices and other vendor devices supporting the L2TPv3 protocol.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
l2tpv3 [hostname <HOSTNAME>|inter-tunnel-bridging|manual-session|
          router-id [<1-4294967295>|<IP>]|tunnel|udp-listen-port
<1024-65535>]
```

Parameters

```
l2tpv3 [hostname <HOSTNAME>|inter-tunnel-bridging|manual-session|
router-id [<1-4294967295>|<IP>]|tunnel|udp-listen-port <1024-65535>]
```

l2tpv3	Configures the L2TPv3 protocol settings for a profile
hostname <HOSTNAME>	Configures the host name sent in the L2TPv3 signalling messages. Tunnel establishment involves exchanging 3 message types (SCCRQ, SCCRP and SCCN) with the peer. Tunnel IDs and capabilities are exchanged during the tunnel establishment with the host. • <HOSTNAME> – Specify the L2TPv3 specific host name.

inter-tunnel-bridging	Enables inter tunnel bridging of packets. This feature is disabled by default.
manual-session	Creates/modifies L2TPv3 manual sessions For more information, see *l2tpv3-manual-session-commands*.
router-id [<1-4294967295>| <IP>]	Configures the router ID sent in the L2TPv3 signalling messages <1-4294967295> – Configures the router ID in decimal format from 1 - 4294967295 <IP> – Configures the router ID in the IP address (A.B.C.D) format
tunnel	Creates/modifies a L2TPv3 tunnel For more information, see *l2tpv3-tunnel-commands*.
udp-listen-port <1024-65535>	Configures the UDP port used to listen for incoming traffic <1024-65535> – Specify the UDP port from 1024 - 65535 (default is 1701)

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#l2tpv3 hostname l2tpv3Host1

rfs7000-37FABE(config-profile-default-rfs7000)#l2tpv3 inter-tunnel-bridging

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
 ..............................................
  l2tpv3 hostname l2tpv3Host1
 l2tpv3 inter-tunnel-bridging
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Negates a L2TPv3 tunnel settings on this profile

l3e-lite-table

Profile Config Commands

Configures L3e lite table aging time

The L3e Lite table stores information about destinations and their location within a specific IPSec tunnel. This enables quicker packet transmissions. The table is updated as nodes transmit packets.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
l3e-lite-table aging-time <10-1000000>
```

Parameters

```
l3e-lite-table aging-time <10-1000000>
```

aging-time <10-1000000>	Configures the aging time in seconds. The aging time defines the duration a learned L3e entry (IP, VLAN) remains in the L3e Lite table before deletion due to lack of activity.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#l3e-lite-table aging-time 1000

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
.....................................................
  interface ge4
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface pppoe1
 use firewall-policy default
 l3e-lite-table aging-time 1000
--More--
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Removes the L3e lite table aging time configuration

led

Profile Config Commands

Turns on and off access point LEDs

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
led {flash-pattern}
```

Parameters

```
led {flash-pattern}
```

flash-pattern	Optional. Enables LED flashing on the device using this profile Select this option to flash an access point's LEDs in a distinct manner (different from its operational LED behavior). Enabling this feature allows an administrator to validate an access point has received its configuration (perhaps remotely at the site of deployment) without having to log into the managing controller or service platform. This feature is disabled by default.

Example

```
rfs7000-37FABE(config-profile-Brocade Mobility RFS7000Test)#led flash-pattern
rfs7000-37FABE(config-profile-Brocade Mobility RFS7000Test)#

rfs7000-37FABE(config-profile-Brocade Mobility RFS7000Test)#show context
profile rfs7000 Brocade Mobility RFS7000Test
 no autoinstall configuration
 no autoinstall firmware
 led flash-pattern
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 --More--
rfs7000-37FABE(config-profile-Brocade Mobility RFS7000Test)#
```

Related Commands:

no	Disables or reverts settings to their default

led-timeout

Profile Config Commands

Configures the LED-timeout timer in the device or profile configuration mode

Supported in the following platforms:

- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
led-timeout [<15-1440>|shutdown]
```

Parameters

```
led-timeout [<15-1440>|shutdown]
```

led-time [<15-1440>| shutdown]	Sets the LED-timeout timer. The value provided here determines the interval (time to lapse) for which a device's LEDs are turned off after the last radio state change. For example, if set at 15 minutes, the LEDs are turned off for 15 minutes after the last radio state change. • <15-1440> – Specify a value from 15 - 1400 minutes. • shutdown – Shutsdown the LED-timeout timer. The device LEDs are not turned off.

Example

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#led-timeout 25
```

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show context
nx9000 B4-C7-99-6C-88-09
 use profile default-nx9000
 use rf-domain default
 hostname nx9500-6C8809
 license AAP
66069c24b3bb1259b34ff016c723a9e299dd408f0ff891e7c5f7e279a382648397d6b3e975e35
6a1
 license HTANLT
66069c24b3bb1259eb36826cab3cc83999dd408f0ff891e74b62b2d3594f0b3dde7967f30e49e
497
 no autogen-uniqueid
 ip default-gateway 192.168.13.2
 led-timeout 25
 --More--
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#

nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#led-timeout shutdown

nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show context
nx9000 B4-C7-99-6C-88-09
 use profile default-nx9000
 use rf-domain default
 hostname nx9500-6C8809
 license AAP
66069c24b3bb1259b34ff016c723a9e299dd408f0ff891e7c5f7e279a382648397d6b3e975e35
6a1
 license HTANLT
66069c24b3bb1259eb36826cab3cc83999dd408f0ff891e74b62b2d3594f0b3dde7967f30e49e
497
 no autogen-uniqueid
 ip default-gateway 192.168.13.2
 led-timeout shutdown
 crypto ikev2 peer IKEv2Peer1
--More--
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
```

Related Commands:

no	Disables LED-timeout timer

legacy-auto-downgrade

Profile Config Commands

Enables device firmware to auto downgrade when legacy devices are detected

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
legacy-auto-downgrade
```

Parameters

None

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#legacy-auto-downgrade
```

Related Commands:

no	Prevents device firmware from auto downgrading when legacy devices are detected

legacy-auto-update

Profile Config Commands

Auto updates an Brocade Mobility 650 Access Point or Brocade Mobility 71XX Access Point legacy access point firmware

Supported in the following platforms:

- Access Points —Brocade Mobility 650 Access Point, Brocade Mobility 7131 Access Point

Syntax:

```
legacy-auto-update [br650|br71xx image <FILE>]
```

Parameters

```
legacy-auto-update [br650|br71xx image <FILE>]
```

legacy-auto-update	Updates a legacy Brocade Mobility 650 Access Point or Brocade Mobility 7131 Access Point access point firmware
br650	Auto updates legacy Brocade Mobility 650 Access Point firmware
br71xx image <FILE>	Auto updates legacy Brocade Mobility 7131 Access Point firmware • image – Sets the path to the firmware image • <FILE> – Specify the path and filename in the flash:/br.img format.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#legacy-auto-update br71xx
image flash:/ap47d.img
```

Related Commands:

no	Disables automatic legacy firmware upgrade

lldp

Profile Config Commands

Configures LLDP settings

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
lldp [holdtime|med-tlv-select|run|timer]

lldp [holdtime <10-1800>|run|timer <5-900>]

lldp med-tlv-select [inventory-management|power-management]
```

Parameters

```
lldp [holdtime <10-1800>|run|timer <5-900>]
```

holdtime <10-1800>	Sets the holdtime for transmitted LLDP PDUs. This command specifies the time a receiving device holds information before discarding it. • <10-1800> – Specify a holdtime from 10 - 1800 seconds.
run	Enables LLDP
timer <5-900>	Sets the transmit interval. This command specifies the transmission frequency of LLDP updates in seconds. • <5-900> – Specify transmit interval from 5 - 900 seconds.

```
lldp med-tlv-select [inventory-management|power-management]
```

med-tlv-select [inventory-management| power-management]	Provides additional media endpoint device TLVs to enable inventory and power management discovery. Specifies the LLDP MED TLVs to send or receive. • inventory-management – Enables inventory management discovery. Allows an endpoint to convey detailed inventory information about itself. • power-management – Enables extended power via MDI discovery. Allows endpoints to convey power information, such as how the device is powered, power priority etc.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#lldp timer 20

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 bridge vlan 1
 ......................................
 use firewall-policy default
 ip dns-server-forward
 ip nat pool pool1
  address range 172.16.10.2 172.16.10.8
 ip nat inside source list test interface vlan1 pool pool1 overload
 lldp timer 20
 --More--
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Disables LLDP on this profile

load-balancing

Profile Config Commands

Configures load balancing parameters

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
load-balancing [advanced-params|balance-br-loads|balance-band-loads|
          balance-channel-loads|band-control-startegy|band-ratio|group-id|
          neighbor-selection-strategy]

load-balancing advanced-params
[2.4GHz-load|5GHz-load|br-load|equality-margin|

hiwater-threshold|max-neighbors|max-preferred-band-load|min-common-clients|
          min-neighbor-rssi|min-probe-rssi]

load-balancing advanced-params [2.4GHz-load|5GHz-load|br-load]
[client-weightage|
          throughput-weightage] <0-100>
load-balancing advanced-params equality-margin [2.4GHz|5GHz|br|band] <0-100>
load-balancing advanced-params hiwater-threshold
[br|channel-2.4GHz|channel-5GHz]
          <0-100>
load-balancing advanced-params max-preferred-band-load [2.4GHz|5GHz] <0-100>
load-balancing advanced-params [max-neighbors <0-16>|min-common-clients
<0-256>|
          min-neighbor-rssi <-100-30>|min-probe-rssi <-100-30>]

load-balancing [balance-br-loads|balance-band-loads|
          balance-channel-loads [2.4GHz|5GHz]]

load-balancing band-control-strategy
[distribute-by-ratio|prefer-2.4GHz|prefer-5GHz]

load-balancing band-ratio [2.4GHz|5GHz] [0|<1-10>]

load-balancing group-id <GROUP-ID>

load-balancing neighbor-selection-strategy
[use-common-clients|use-roam-notification|
          use-smart-rf|use-wips]
```

Parameters

	`load-balancing advanced-params [2.4GHz-load|5GHz-load|br-load] [client-weightage| throughput-weightage] <0-100>`
advanced-params	Configures advanced load balancing parameters
2.4GHz-load [client-weightage| throughput-weightage] <0-100>	Configures 2.4 GHz load calculation weightages • client-weightage – Specifies weightage assigned to the client-count when calculating the 2.4 GHz load • throughput-weightage – Specifies weightage assigned to throughput, when calculating the 2.4 GHz band, channel, or radio load The following keyword is common to the 'client-weightage' and 'throughput-weightage' parameters: • <0-100> – Sets the margin as a load percentage from 1 - 100
5GHz-load [client-weightage| throughput-weightage] <0-100>	Configures 5.0 GHz load calculation weightages • client-weightage – Specifies weightage assigned to the client-count when calculating the 5.0 GHz load • throughput-weightage – Specifies weightage assigned to throughput, when calculating the 5.0 GHz band, channel or radio load The following keyword is common to the 'client-weightage' and 'throughput-weightage' parameters: • <0-100> – Sets the margin as a load percentage from1 - 100
br-load [client-weightage| throughput-weightage] <0-100>	Configures AP load calculation weightages • client-weightage – Specifies weightage assigned to the client-count, when calculating the AP load • throughput-weightage – Specifies weightage assigned to throughput, when calculating the AP load The following keyword is common to the 'client-weightage' and 'throughput-weightage' parameters: • <0-100> – Sets the margin as a load percentage from 1 - 100

	`load-balancing advanced-params equality-margin [2.4GHz|5GHz|br|band] <0-100>`
advanced-params	Configures advanced load balancing parameters
equality-margin [2.4GHz|5GHz|br|band] <0-100>	Configures the maximum load difference considered equal. The load is compared for different 2.4 GHz channels, 5.0 GHz channels, AP, or bands. • 2.4GHz – Configures the maximum load difference considered equal when comparing loads on different 2.4 GHz channels • 5GHz – Configures the maximum load difference considered equal when comparing loads on different 5.0 GHz channels • br – Configures the maximum load difference considered equal when comparing loads on different APs • band – Configures the maximum load difference considered equal when comparing loads on different bands The following keyword is common to 2.4 GHz channels, 5.0 GHz channels, APs, and bands: • <0-100> – Sets the margin as a load percentage from 1 - 100

	`load-balancing advanced-params hiwater-threshold [br|channel-2.4GHz|channel-5GHz] <0-100>`
advanced-params	Configures advanced load balancing parameters
hiwater-threshold	Configures the load beyond which load balancing is invoked
[br|channel-2.4GHz| channel-5GHz] <0-100>	Select one of the following options: • br – Configures the AP load beyond which load balancing begins • channel-2.4GHz – Configures the AP load beyond which load balancing begins (for APs on 2.4 GHz channel) • channel-5GHz – Configures the AP load beyond which load balancing begins for (APs on 5.0 GHz channel) The following keyword is common for the 'AP', 'channel-2.4GHz', and 'channel-5GHz' parameters: • <0-100> – Sets the load threshold as a number from 1 - 100

`load-balancing advanced-params max-preferred-band-load [2.4GHGz|5GHzd] <0-100>`

advanced-params	Configures advanced load balancing parameters
max-preferred-band-load	Configures the maximum load on the preferred band, beyond which the other band is equally preferred
[2.4GHz|5GHz] <0-100>	Select one of the following options: • 2.4GHz – Configures the maximum load on 2.4 GHz, when it is the preferred band • 5GHz – Configures the maximum load on 5.0 GHz, when it is the preferred band The following keyword is common to the 2.4 GHz and 5.0 GHz bands: • <0-100> – Configures the maximum load as a percentage from 0 - 100

`load-balancing advanced-params [max-neighbors <0-16>|min-common-clients <0-256>|`
`min-neighbor-rssi <-100-30>|min-probe-rssi <-100-30>]`

advanced-params	Configures advanced load balancing parameters
max-neighbors <0-6>	Configures the maximum number of confirmed neighbors to balance • <0-6> – Specify a value from 0 - 6. Optionally configure a minimum of 0 neighbors and a maximum of 6 neighbors
min-common-clients <0-256>	Configures the minimum number of common clients that can be shared with the neighbor for load balancing • <0-256> – Specify a value from 0 - 256. Optionally configure a minimum of 0 clients and a maximum of 256 clients.
min-neighbor-rssi <-100-30>	Configures the minimum signal strength (*Received Signal Strength Indicator* - RSSI) of a neighbor detected • <-100-30> – Sets the signal strength in dBm. Specify a value from -100 - 30 dBm.
min-probe-rssi <-100-30>	Configures the minimum received probe signal strength required to qualify the sender as a common client • <0-100> – Sets the signal strength in dBm. Specify a value from -100 - 30 dBm.

`load-balancing [balance-br-loads|balance-band-loads|balance-channel-loads [2.4GHz|5GHz]]`

balance-br-loads	Enables neighbor AP load balancing. This option distributes the access point's radio load amongst other controller managed access point radios. This option is enabled by default.
balance-band-loads	Enables balancing of the total band load amongst neighbors. This option balances the access point's radio load by assigning a ratio to both the 2.4 GHz and 5.0 GHz bands. Balancing radio load by band ratio allows an administrator to assign a greater weight to radio traffic on either the 2.4 GHz or 5.0 GHz band. This option is enabled by default.
balance-channel-loads [2.4GHz|5GHz]	Enables the following: • 2.4GHz – Channel load balancing on 2.4 GHz band Balances the access point's 2.4 GHz radio load across channels supported within the country of deployment. This can prevent congestion on the 2.4 GHz radio if a channel is over utilized. • 5GHz – Channel load balancing on 5.0 GHz band Balances the access point's 5.0 GHz radio load across channels supported within the country of deployment. This can prevent congestion on the 5.0 GHz radio if a channel is over utilized.

`load-balancing band-control-strategy`
`[distribute-by-ratio|prefer-2.4GHz|prefer-5GHz]`

band-control-strategy	Configures a band control strategy
distribute-by-ratio	Distributes clients to either band according to the band-ratio
prefer-2.4GHz	Nudges all dual-band clients to 2.4 GHz band
prefer-5GHz	Nudges all dual-band clients to 5.0 GHz band

load-balancing band-ratio [2.4GHz|5GHz] [0|<1-10>]	
band-ratio	Configures the relative loading of 2.4 GHz band and 5.0 GHz band.This allows an administrator to weight client traffic load if wishing to prioritize client traffic load on the 2.4 GHz or the radio band. The higher the value set, the greater the weight assigned to radio traffic load on the 2.4 GHz or 5.0 GHz radio band.
2.4GHz [0|<1-10>]	Configures the relative loading of 2.4 GHz band • 0 – Selecting '0' steers all dual-band clients preferentially to the other band • <0-10> – Configures a relative load as a number from 0 - 10. The default is 1.
5ghz [0|<1-10>]	Configures the relative loading of 5.0 GHz band • 0 – Selecting '0' steers all dual-band clients preferentially to the other band • <0-10> – Configures a relative load as a number from 0 - 10. The default is 1.

load-balancing group-id <GROIP-ID>	
group-id <GROUP-ID>	Configures group ID to facilitate load balancing • <GROUP-ID> – Specify the group ID.

load-balancing neighbor-selection-strategy [use-common-clients|use-roam-notification| use-smart-rf]	
neighbor-selection-strategy	Configures a neighbor selection strategy. The options are: use-common-clients, use-roam-notification, and use-smart-rf
use-common-clients	Selects neighbors based on probes from clients common to neighbors
use-roam-notification	Selects neighbors based on roam notifications from roamed clients
use-smart-rf	Selects neighbors detected by Smart RF

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#load-balancing advanced-params
2.4ghz-load throughput-weightage 90

rfs7000-37FABE(config-profile-default-rfs7000)#load-balancing advanced-params
hiwater-threshold br 90

rfs7000-37FABE(config-profile-default-rfs7000)#load-balancing
balance-br-loads

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
 ip default-gateway 172.16.10.4
 autoinstall configuration
 autoinstall firmware
 load-balancing advanced-params 2.4ghz-load throughput-weightage 90
 load-balancing advanced-params hiwater-threshold br 90
 load-balancing balance-br-loads
--More--
rfs7000-37FABE(config-profile-default-rfs7000)#s
```

Related Commands:

no	Disables load balancing on this profile

logging

Profile Config Commands

Enables message logging and configures logging settings

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
logging [aggregation-time|buffered|console|facility|forward|host|on|syslog]

logging [aggregation-time <1-60>|host <IP>|on]
logging [buffered|console|syslog|forward]
[<0-7>|emergencies|alerts|critical|errors|
          warnings|notifications|informational|debugging]
logging facility [local0|local1|local2|local3|local4|local5|local6|local7]
```

Parameters

```
logging [aggregation-time <1-60>|host <IP>|on]
```

aggregation-time <1-60>	Sets the number of seconds for aggregating repeated messages • <1-60> – Specify a value from 1 - 60 seconds.
host <IP>	Configures a remote host to receive log messages. Defines numerical (non DNS) IP addresses for external resources where logged system events can be sent on behalf of the controller profile. • <IP> – Specify the IP address of the remote host.
on	Enables the logging of system messages

```
logging [buffered|console|syslog|forward] [<0-7>|emergencies|alerts|critical|
errors|warnings|notifications|informational|debugging]
```

buffered	Sets the buffered logging level
console	Sets the console logging level
syslog	Sets the syslog server's logging level
forward	Forwards system debug messages to the wireless controller or service platform

[<0-7>|alerts| criticail|debugging| emergencies|errors| informational| notifications| warnings]	The following keywords are common to the buffered, console, syslog, and forward parameters. All incoming messages have different severity levels based on their importance. The severity level is fixed on a scale of 0 - 7. • <0-7> – Sets the message logging severity level on a scale of 0 - 7 • emergencies – Severity level 0: System is unusable • alerts – Severity level 1: Requires immediate action • critical – Severity level 2: Critical conditions • errors – Severity level 3: Error conditions • warnings – Severity level 4: Warning conditions (default) Contd..
	• notifications – Severity level 5: Normal but significant conditions • informational – Severity level 6: Informational messages • debugging – Severity level 7: Debugging messages
	`logging facility [local0|local1|local2|local3|local4|local5|local6|local7]`
facility [local0|local1| local2|local3|local4| local5|local6|local7]	Enables the syslog to decide where to send the incoming message. There are 8 logging facilities, from syslog0 to syslog7. • local0 – Syslog facility local0 • local1 – Syslog facility local1 • local2 – Syslog facility local2 • local3 – Syslog facility local3 • local4 – Syslog facility local4 • local5 – Syslog facility local5 • local6 – Syslog facility local6 • local7 – Syslog facility local7

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#logging facility local4

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 bridge vlan 1
 ................................................
 ip dns-server-forward
 logging facility local4
 ip nat pool pool1
  address range 172.16.10.2 172.16.10.8
 ip nat inside source list test interface vlan1 pool pool1 overload
 lldp timer 20
service pm sys-restart
 router ospf
 l2tpv3 hostname l2tpv3Host1
 l2tpv3 inter-tunnel-bridging
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Disables logging on this profile

mac-address-table

Profile Config Commands

Configures the MAC address table. Use this command to assign a static address to the MAC address table.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
mac-address-table [aging-time|static]
mac-address-table aging-time [0|<10-1000000>]
mac-address-table static <MAC> vlan <1-4094> interface [<L2-INTERFACE>|ge
<1-4>|
          port-channel <1-2>]
```

Parameters

```
mac-address-table aging-time [0|<10-1000000>]
```

aging-time [0|<10-1000000>]	Sets the duration a learned MAC address persists after the last update • 0 – Entering the value '0' disables the aging time • <10-1000000> – Sets the aging time from 10 -100000 seconds

```
mac-address-table static <MAC> vlan <1-4094> interface [<L2-INTERFACE>|ge
<1-4>|
port-channel <1-2>]
```

static <MAC>	Creates a static MAC address table entry • <MAC> – Specifies the static address to add to the MAC address table. Specify the MAC address in the AA-BB-CC-DD-EE-FF, AA:BB:CC:DD:EE:FF, or AABB.CCDD.EEFF format.
vlan <1-4094>	Assigns a static MAC address to a specified VLAN port • <1-4094> – Specify the VLAN index from 1 - 4094.

interface [<L2-INTERFACE>| ge <1-4>| port-channel <1-2>]	Specifies the interface type. The options are: layer 2 Interface, GigabitEthernet interface, and a port channel interface
	• <L2-INTERFACE> – Specify the layer 2 interface name.
	• ge – Specifies a GigabitEthernet interface
	  • <1-4> – Specify the GigabitEthernet interface index from 1 - 4.
	• port-channel – Specifies a port channel interface
	  • <1-2> – Specify the port channel interface index from 1 - 2.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#mac-address-table static
00-40-96-B0-BA-2A vlan 1 interface ge 1

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 bridge vlan 1
.....................................................
  logging facility local4
 mac-address-table static 00-40-96-B0-BA-2A vlan 1 interface ge1
 ip nat pool pool1
--More--
```

```
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Disables or reverts settings to their default

mac-auth

Profile Config Commands

Enables or disables authentication of a client's MAC address on wired ports. When configured, MAC authentication will be enabled on devices using this profile.

To enable MAC address authentication on a device, enter the device's configuration mode and execute the *mac-auth* command.

When enabled, the source MAC address of a device, connected to the specified wired port, is authenticated with the RADIUS server. Once authenticated the device is permitted access to the managed network and packets from the authenticated source are processed. If not authenticated the device is either denied access or provided guest access through the guest VLAN (provided guest VLAN access is configured on the port).

Enabling MAC authentication requires you to first configure a AAA policy specifying the RADIUS server. Configure the client's MAC address on the specified RADIUS server. Attach this AAA policy to a profile or a device. Finally, enable MAC authentication on the desired wired port of the device or device-profile.

Only one MAC address is supported for every wired port. Consequently, when one source MAC address is authenticated, packets from all other sources are dropped.

To enable client MAC authentication on a wired port:

1. Configure the user on the RADIUS server. The following examples create a RADIUS server user entry.

   a. `<DEVICE>(config)#radius-group <RAD-GROUP-NAME>`

      `<DEVICE>(config-radius-group-<RAD-GROUP-NAME>)#policy vlan <VLAN-ID>`

   b. `<DEVICE>(config)#radius-user-pool-policy <RAD-USER-POOL-NAME>`

      `<DEVICE>(config-radius-user-pool-<RAD-USER-POOL-NAME>)#user <USER-NAME> password <PASSWORD> group <RAD-GROUP-OF-STEP-A>`

      Note: The <USER-NAME> and <PASSWORD> should be the client's MAC address. This address will be matched against the MAC address of incoming traffic at the specified wired port.

   c. `<DEVICE>(config)#radius-server-policy <RAD-SERVER-POL-NAME>`

      `<DEVICE>(config-radius-server-policy-<RAD-SERVER-POL-NAME>)#use radius-user-pool-policy <RAD-USER-POOL-OF-STEP-B>`

2. Configure a AAA policy exclusively for wired MAC authentication and specify the authentication (RADIUS) server settings. The following example creates a AAA policy 'macauth' and enters its configuration mode:

   ```
   <DEVICE-A>(config)#aaa-policy macauth
   <DEVICE-A>(config-aaa-policy-macauth)#...
   ```

   Specify the RADIUS server details.

```
<DEVICE-A>(config)#aaa-policy macauth
<DEVICE-A>(config-aaa-policy-macauth)#authentication server <1-6> [host
<IP>|onboard]
```

Attach the AAA policy to the device or profile. When attached to a profile, the AAA policy is applied to all devices using this profile.

```
<DEVICE>(config-device-aa-bb-cc-dd-ee)#mac-auth use aaa-policy macauth

<DEVICE>(config-profile-<DEVICE-PROFILE-NAME>)#mac-auth use aaa-policy
macauth
```

3. Enable mac-auth on the device's desired GE port. When enabled on a profile, MAC address authentication is enabled, on the specified GE port, of all devices using this profile.

```
<DEVICE>(config-device-aa-bb-cc-dd-ee)#interface ge x
<DEVICE>(config-device-aa-bb-cc-dd-ee-gex)#mac-auth

<DEVICE>(config-profile-<PROFILE-NAME>)#interface ge x
<DEVICE>(config-profile-<PROFILE-NAME>)#mac-auth
```

Supported in the following platforms:

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
mac-auth use aaa-policy <AAA-POLICY-NAME>
```

Parameters

```
mac-auth use aaa-policy <AAA-POLICY-NAME>
```

mac-auth	Enables 802.1X authentication of MAC addresses on this profile. Use the device configuration mode to enable this feature on a device.
use aaa-policy <AAA-POLICY-NAME>	Associates an existing AAA policy with this profile (or device) • <AAA-POLICY NAME> – Specify the AAA policy name. The AAA policy used should be created especially for MAC authentication.

Example

```
The following examples demonstrate the configuration of authentication of MAC
addresses on wired ports:

rfs4000-229D58(config-aaa-policy-mac-auth)#authentication server 1 onboard
controller

rfs4000-229D58(config-aaa-policy-mac-auth)#show context
aaa-policy mac-auth
 authentication server 1 onboard controller
rfs4000-229D58(config-aaa-policy-mac-auth)#

rfs4000-229D58(config)#radius-group RG
rfs4000-229D58(config-radius-group-RG)#policy vlan 11

rfs4000-229D58(config-radius-group-RG)#show context
radius-group RF
 policy vlan 11
rfs4000-229D58(config-radius-group-RG)#
```

```
rfs4000-229D58(config)#radius-user-pool-policy RUG
rfs4000-229D58(config-radius-user-pool-RUG)#user 00-16-41-55-F8-5D password 0
0-16-41-55-F8-5D group RG

rfs4000-229D58(config-radius-user-pool-RUG)#show context
radius-user-pool-policy RUG
 user 00-16-41-55-F8-5D password 0 00-16-41-55-F8-5D group RG
rfs4000-229D58(config-radius-user-pool-RUG)#

rfs4000-229D58(config)#radius-server-policy RS
rfs4000-229D58(config-radius-server-policy-RS)#use radius-user-pool-policy
RUG

rfs4000-229D58(config-radius-server-policy-RS)#show context
radius-server-policy RS
 use radius-user-pool-policy RUG
rfs4000-229D58(config-radius-server-policy-RS)#

rfs4000-229D58(config-device-00-23-68-22-9D-58-if-ge4)#show context
 interface ge4
  dot1x authenticator host-mode single-host
  dot1x authenticator port-control auto
  mac-auth
rfs4000-229D58(config-device-00-23-68-22-9D-58-if-ge4)#

rfs4000-229D58(config-device-00-23-68-22-9D-58-if-ge5)#show context
 interface ge5
  switchport mode access
  switchport access vlan 1
  dot1x authenticator host-mode single-host
  dot1x authenticator guest-vlan 5
  dot1x authenticator port-control auto
  mac-auth
rfs4000-229D58(config-device-00-23-68-22-9D-58-if-ge5)#

rfs4000-229D58(config-device-00-23-68-22-9D-58)#show macauth interface ge 4
Mac Auth info for interface GE4
-----------------------------------
 Mac Auth Enabled
 Mac Auth Authorized
Client MAC 00-16-41-55-F8-5D

rfs4000-229D58(config-device-00-23-68-22-9D-58)#

rfs4000-229D58(config-device-00-23-68-22-9D-58)#show macauth interface ge 5
Mac Auth info for interface GE5
-----------------------------------
 Mac Auth Enabled
 Mac Auth Not Authorized

rfs4000-229D58(config-device-00-23-68-22-9D-58)#
```

Related Commands:

no	Disables authentication of MAC addresses on wired ports settings on this profile (or device)

memory-profile

Profile Config Commands

Configures memory profile used on the device

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
memory-profile [adopted|standalone]
```

Parameters

```
memory-profile [adopted|standalone]
```

adopted	Configures adopted mode (no GUI and higher MiNT routes, firewall flows)
standalone	Configures standalone mode (GUI and fewer MiNT routes, firewall flows)

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#memory-profile adopted
% Error on default-rfs7000: memory-profile is not supported on this device
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Resets device's memory profile configuration

meshpoint-device

Profile Config Commands

Configures meshpoint device parameters. This feature is configurable in the profile and device configuration modes.

Supported in the following platforms:

- Access Points — Brocade Mobility 71XX Access Point

Syntax:

```
meshpoint-device <MESHPOINT-NAME>
```

Parameters

```
meshpoint-device <MESHPOINT-NAME>
```

meshpoint-device <MESHPOINT-NAME>	Configures meshpoint device parameters • <MESHPOINT-NAME> – Specify meshpoint name.

Usage Guidelines:

For *Vehicular Mounted Modem* (VMM) access points or other mobile devices, set the path selection method as mobile-snr-leaf in the config-meshpoint-device mode. For more information, see *path-method*.

Example

```
rfs7000-37FABE(config-profile-testBrocade Mobility 71XX Access
Point)#meshpoint-device test
rfs7000-37FABE(config-profile-testBrocade Mobility 71XX Access
Point-meshpoint-test)#

rfs7000-37FABE(config-profile-testBrocade Mobility 71XX Access
Point-meshpoint-test)#?
Mesh Point Device Mode commands:
  acs           Configure auto channel selection parameters
  exclude       Exclude neighboring Mesh Devices
  hysteresis    Configure path selection SNR hysteresis values
  monitor       Event Monitoring
  no            Negate a command or set its defaults
  path-method   Path selection method used to find a root node
  preferred     Configure preferred path parameters
  root          Set this meshpoint as root

  clrscr        Clears the display screen
  commit        Commit all changes made in this session
  do            Run commands from Exec mode
  end           End current mode and change to EXEC mode
  exit          End current mode and down to previous mode
  help          Description of the interactive help system
  revert        Revert changes
  service       Service Commands
  show          Show running system information
  write         Write running configuration to memory or terminal

rfs7000-37FABE(config-profile-testBrocade Mobility 71XX Access
Point-meshpoint-test)#
```

Related Commands:

no	Removes a specified meshpoint

NOTE
For more information on the meshpoint-device configuration parameters, see *Chapter 27, <$elemtextMESHPOINT*.

meshpoint-monitor-interval

Profile Config Commands

Configures the meshpoint monitoring interval. This is the interval, in seconds, the up/down status of a meshpoint is checked.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
meshpoint-monitor-interval <1-65535>
```

Parameters

```
meshpoint-monitor-interval <1-65535>
```

meshpoint-monitor-interval <1-65535>	Configures the meshpoint monitoring interval in seconds • <1-65535> – Specify the interval from 1 - 65535 seconds. The default is 30 seconds.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#meshpoint-monitor-interval 100

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
 meshpoint-monitor-interval 100
 ip default-gateway 172.16.10.4
 --More--
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Resets the meshpoint monitoring interval to default (30 seconds)

min-misconfiguration-recovery-time

Profile Config Commands

Configures the minimum device connectivity verification time

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
min-misconfiguration-recovery-time <60-3600>
```

Parameters

```
min-misconfiguration-recovery-time <60-3600>
```

min-misconfiguration-recovery -time <60-3600>	Configures the minimum connectivity (with the associated device) verification interval • <60-3600> – Specify a value from 1 - 3600 seconds (default is 60 seconds).

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#min-misconfiguration-recovery-
time 200
% Error on default-rfs7000: Unknown config-item (id:min_misconf_recovery_time)
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Resets setting to default (60 seconds)

mint

Profile Config Commands

Configures MiNT protocol commands

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
mint [dis|level|link|mlcp|spf-latency|tunnel-controller-load-balancing]

mint dis [priority-adjustment <-255-255>|strict-evis-reachability]

mint level 1 area-id <1-16777215>

mint link [force|ip|listen|vlan]

mint link force ip <IP> [<1-65535>|level]
mint link force ip <IP> [<1-65535> level 2|level 2] {adjacency-hold-time
<2-600>|
          cost <1-10000>|hello-interval <1-120>|ipsec-secure {gw}}

mint link [listen ip <IP>|vlan <1-4094>] {adjacency-hold-time <2-600>|cost
<1-10000>|
          hello-interval <1-120>|ipsec-security {gw}|level [1|2]}

mint link ip <IP> {<1-65535>|adjacency-hold-time <2-600>|cost <1-10000>|
          hello-interval <1-120>|ipsec-security {gw}|level [1|2]}

mint mlcp [ip|vlan]

mint spf-latency <0-60>
```

```
mint tunnel-controller-load-balancing level1
```

Parameters

```
mint dis [priority-adjustment <-255-255>|strict-evis-reachability]
```

dis priority-adjustment <-255-255>	Sets the relative priority for the router to become DIS (designated router) • priority-adjustment – Sets priority adjustment added to base priority • <-255-255> – Specify a value from -255 - 255. The default is 0. Higher numbers result in higher priorities
strict-evis-reachability	Enables reaching EVIS election winners through MiNT

```
mint level 1 area-id <1-16777215>
```

level 1	Configures local MiNT routing settings • 1 – Configures local MiNT routing level
area-id <1-16777215>	Specifies the routing area identifier • <1-16777215> – Specify a value from 1 - 16777215.

```
mint link force ip <IP> [<1-65535> level 2|level 2] {adjacency-hold-time
<2-600>|
cost <1-10000>|hello-interval <1-120>|ipsec-security {gw}}
```

link force	Creates a MiNT routing link • force – Forces a MiNT routing link to be created even if not necessary
ip <IP>	Creates a MiNT tunnel over UDP/IP • <IP> – Specify peer's IP address
<1-65535> level 2	Specifies a peer's UDP port to link with the specified IP address • level – Specifies routing level • 2 – Configures inter-site MiNT routing level
adjacent-hold-time <2-600>	Optional. Specifies the adjacency lifetime after hello packets cease • <2-600> – Specify a value from 2 - 600 seconds.
cost <1-100000>	Optional. Specifies the link cost in arbitrary units • <1-100000> – Specify a value from 1 - 100000.
hello-interval <1-120>	Optional. Specifies the hello-interval between packets • <1-120> – Specify a value from 1 - 120 seconds.
ipsec-security {gw}	Optional. Configures the IPSec security gateway

```
mint link [listen ip <IP>|vlan <1-4094>] {adjacency-hold-time <2-600>|cost
<1-10000>|
hello-interval <1-120>|level [1|2]|ipsec-security {gw}}
```

link listen ip <IP>	Creates a MiNT routing link • listen – Creates a MiNT listening link • ip – Creates a MiNT listening link over UDP/IP • <IP> – Specify the IP address of the listening port.
vlan <1-4094>	Enables MiNT routing on VLAN • <1-4094> – Select VLAN ID from 1 - 4094.
adjacent-hold-time <2-600>	Optional. Specifies the adjacency lifetime after hello packets cease • <2-600> – Specify a value from 2 - 600 seconds.

cost <1-100000>	This parameter is common to the 'listen' and 'vlan' parameters: • Optional. Specifies the link cost in arbitrary units • <1-100000> – Specify a value from 1 - 100000.
hello-interval <1-120>	This parameter is common to the 'listen' and 'vlan' parameters: • Optional. Specifies the interval between hello packets • <1-120> – Specify a value from 1 - 120.
level [1|2]	This parameter is common to the 'listen' and 'vlan' parameters: Optional. Specifies the routing levels for this routing link. The options are: • 1 – Configures local routing • 2 – Configures inter-site routing
ipsec-security {gw}	This parameter is common to the 'listen' and 'vlan' parameters: • gw – Optional. Configures the IPSec security gateway

```
mint link ip <IP> {<1-65535>|adjacency-hold-time <2-600>|cost <1-10000>|
hello-interval <1-120>|level [1|2]|ipsec-security {gw}}
```

link ip <IP>	Creates a MiNT routing link • ip – Creates a MiNT tunnel over UDP/IP • <IP> – Specify the IP address of the peer.
<1-65535>	Select the peer UDP port from 1 - 65535.
adjacent-hold-time <2-600>	Optional. Specifies the adjacency lifetime after hello packets cease • <2-600> – Specify a value from 2 - 600 seconds.
cost <1-100000>	Optional. Specifies the link cost in arbitrary units • <1-100000> – Specify a value from 1 - 100000.
hello-interval <1-120>	Optional. Specifies the hello interval between packets <1-120> – Specify a value from 1 - 120.
level [1|2]	Optional. Specifies the routing levels for this routing link. The options are: • 1 – Configures local routing • 2 – Configures inter-site routing
ipsec-security {gw}	Optional. Configures the IPSec security gateway

```
mint mlcp [ip|vlan]
```

mlcp [ip|vlan]	Configures the *MiNT Link Creation Protocol* (MLCP) • vlan – Configures MLCP over layer 2 (VLAN) links • ip – Configures MLCP over layer 3 (UDP/IP) links

```
mint spf-latency <0-60>
```

spf-latency <0-60>	Specifies the latency of SPF routing recalculation • <0-60> – Specify the latency from 0 - 60 seconds.

```
mint tunnel-controller-load-balancing level1
```

tunnel-controller-load-balancing level1	Configures load balancing of MiNT extended VLAN traffic across tunnels • level1 – Enables balancing of load of a tunnel wireless controller or service platform over VLAN links

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#mint level 1 area-id 88

rfs7000-37FABE(config-profile-default-rfs7000)#mint link ip 1.2.3.4 level 1

rfs7000-37FABE(config-profile-default-rfs7000)#show context
```

```
profile rfs7000 default-rfs7000
 mint link ip 1.2.3.4
 mint level 1 area-id 88
 bridge vlan 1
--More--
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Disables or reverts settings to their default

misconfiguration-recovery-time

Profile Config Commands

Verifies connectivity after a configuration is received

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
misconfiguration-recovery-time [0|<60-300>]
```

Parameters

```
misconfiguration-recovery-time [0|<60-300>]
```

<60-300>	Sets the recovery time from 60 - 300 seconds (default is 180 seconds)
0	Disables recovery from misconfiguration

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#misconfiguration-recovery-time
65

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 mint link ip 1.2.3.4
 mint level 1 area-id 88
 bridge vlan 1
  bridging-mode isolated-tunnel
  ..............................................
  qos trust 802.1p
 interface pppoe1
 use firewall-policy default
 misconfiguration-recovery-time 65
service pm sys-restart
 router ospf
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Reverts to default (180 seconds)

neighbor-inactivity-timeout

Profile Config Commands

Configures neighbor inactivity timeout

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
neighbor-inactivity-timeout <1-1000>
```

Parameters

```
neighbor-inactivity-timeout <1-1000>
```

<1-1000>	Sets neighbor inactivity timeout • <1-1000> – Specify a value from 1 - 1000 seconds.

Example

```
rfs7000-37FABE(config-profile-default)#neighbor-inactivity-timeout 500

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 mint link ip 1.2.3.4
 mint level 1 area-id 88
 bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
 neighbor-inactivity-timeout 500
 autoinstall configuration
 autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 interface me1
 interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
```

```
--More--
rfs7000-37FABE(config-profile-default-rfs7000)#
```

neighbor-info-interval

Profile Config Commands

Configures the neighbor information exchange interval

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
neighbor-info-interval <1-100>
```

Parameters

```
neighbor-info-interval <1-100>
```

<1-100>	Sets interval in seconds from 1 - 100

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#neighbor-info-interval 6

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 mint link ip 1.2.3.4
 mint level 1 area-id 88
 bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
 neighbor-info-interval 6
 neighbor-inactivity-timeout 500
 autoinstall configuration
 autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 interface me1
 interface ge1
  ip dhcp trust
  qos trust dscp
--More--
rfs7000-37FABE(config-profile-default-rfs7000)#
```

no

Profile Config Commands

Negates a command or resets values to their default

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no [adopter-auto-provisioning-policy-lookup|alias|area|arp|

auto-learn-staging-config|autogen-uniqueid|autoinstall|bridge|cdp|cluster|

configuration-persistence|controller|critical-resource|crypto|device-upgrade|
dot1x|

dscp-mapping|email-notification|environmental-sensor|events|export|floor|gre|
          http-analyze|interface|ip|l2tpv3|l3e-lite-table|led|led-timeout|

legacy-auto-downgrade|legacy-auto-update|lldp|load-balancing|logging|
          mac-address-table|mac-auth|memory-profile|meshpoint-device|
          meshpoint-monitor-interval|min-misconfiguration-recovery-time|mint|

misconfiguration-recovery-time|noc|ntp|power-config|preferred-controller-grou
p|

preferred-tunnel-controller|radius|rf-domain-manager|router|spanning-tree|
          tunnel-controller|use|vrrp|wep-shared-key-auth|service]
```

Parameters

None

Usage Guidelines:

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#no cluster
```

Related Commands:

adopter-auto-provisioning-policy-lookup	Enables the use of a centralized auto provisioning policy on this profile
alias	Configures network, VLAN, and service aliases on this profile
area	Enables adoption of Brocade Mobility 300 Access Points
area	Sets the area name where the system is located

arp	Configures static address resolution protocol
auto-learn-staging-config	Enables network configuration device learning
autogen-uniqueid	Autogenerates a unique local ID for devices using this profile. When executed in the device configuration mode, this command generates a unique ID for the logged device.
autoinstall	Configures the autoinstall feature
bridge	Configures bridge specific commands
captive-portal	Configures captive portal advanced Web page uploads on a profile or device
cdp	Enables CDP on a device
cluster	Configures a cluster name
configuration-persistence	Enables configuration persistence across reloads
controller	Configures a wireless controller or service platform
critical-resource	Monitors user configured IP addresses and logs their status
crypto	Configures crypto settings
device-upgrade	Configures device firmware upgrade settings on this profile
dot1x	Configures 802.1x standard authentication controls
dscp-mapping	Configures an IP DSCP to 802.1p priority mapping for untagged frames
email-notification	Configures e-mail notification
enforce-version	Enables checking of a device's firmware version before attempting adoption or clustering
environmental-sensor	Configures the environmental sensor device settings
events	Displays system event messages
export	Enables the export of the startup.log file after every boot
floor	Sets the floor name where the system is located
gre	Enables GRE tunneling on this device
http-analyze	Configures HTTP analysis settings
interface	Configures an interface
ip	Configures IP components
l2tpv3	Defines the *Layer 2 Tunnel Protocol* (L2TP) protocol for tunneling layer 2 payloads using VPNs
l3e-lite-table	Configures L3e Lite Table with this profile
led	Turns device LEDs on or off
led-timeout	Configures LED-timeout timer. This command is specific to the NX9000 series service platforms.
legacy-auto-downgrade	Auto downgrades a legacy device firmware
legacy-auto-update	Auto upgrades a legacy device firmware
lldp	Configures *Link Layer Discovery Protocol* (LLDP)
load-balancing	Configures load balancing parameters
logging	Modifies message logging
mac-address-table	Configures the MAC address table
mac-auth	Enables 802.1x port-based user authentication on this device
memory-profile	Configures the memory profile used on the device

meshpoint-device	Configures the meshpoint device parameters
meshpoint-monitor-interval	Configures the meshpoint monitoring interval
min-misconfiguration-recovery-time	Configures the minimum connectivity (with connected device) verification time
mint	Configures the MiNT protocol settings
misconfiguration-recovery-time	Verifies connectivity after a device configuration file is received
neighbor-inactivity-timeout	Configures neighbor inactivity timeout
neighbor-info-interval	Configures the neighbor information exchange interval
noc	Configures NOC settings
ntp	Configures an NTP server
power-config	Configures the power option mode. Sets the amount of power that the access point draws.
preferred-controller-group	Specifies the wireless controller or service platform's group preferred for adoption
preferred-tunnel-controller	Configures the tunnel wireless controller or service platform's name preferred for tunneling extended VLAN traffic
radius	Configures device-level RADIUS authentication parameters
rf-domain-manager	Enables RF Domain manager
router	Configures dynamic router protocol settings
spanning-tree	Enables automatic AP firmware upgrade
tunnel-controller	Configures the tunneled WLAN (extended-VLAN) wireless controller's name
use	Defines the settings used by this feature
vrrp	Configures VRRP group settings
wep-shared-key-auth	Enables support for 802.11 WEP shared key authentication
clrscr	Clears the display screen
commit	Commits (saves) changes made in the current session
end	Ends and exits the current mode and moves to the PRIV EXEC mode
exit	Ends the current mode and moves to the previous mode
help	Displays the interactive help system
revert	Reverts changes to their last saved configuration
service	Invokes service commands to troubleshoot or debug (config-if) instance configurations
show	Displays running system information
write	Writes information to memory or terminal

noc

Profile Config Commands

Configures *Network Operations Center* (NOC) settings, such as NOC statistics update interval

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
noc update-interval [<5-3600>|auto]
```

Parameters

```
noc update-interval [<5-3600>|auto]
```

update-interval [<5-3600>|auto]	Configures NOC statistics update interval • <5-3600> – Specify the update interval from 5 - 3600 seconds. • auto – The NOC statistics update interval is automatically adjusted by the wireless controller or service platform based on load

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#noc update-interval 25

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 mint link ip 1.2.3.4
 mint level 1 area-id 88
 bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
 ................................................
 interface pppoe1
 use firewall-policy default
 misconfiguration-recovery-time 65
 noc update-interval 25
service pm sys-restart
 router ospf
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Resets NOC related parameters

ntp

Profile Config Commands

Configures the *Network Time Protocol* (NTP) server settings

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
ntp server <PEER-IP> {autokey|key|prefer|version}
ntp server <PEER-IP> {autokey} {prefer version <1-4>|version <1-4>}

ntp server <PEER-IP> {key <1-65534> md5 [0 <WORD>|2<WORD>|<WORD>]}
          {prefer version <1-4>|version <1-4>}

ntp server <PEER-IP> {prefer version <1-4>|version <1-4> prefer}
```

Parameters

```
ntp server <PEER-IP> {autokey} {prefer version <1-4>|version <1-4>}
```

server <PEER-IP>	Configures a NTP server association
autokey {prefer version <1-4>| version <1-4>}	Optional. Configures an autokey peer authentication scheme • prefer – Optional. Prefers this peer when possible • version – Optional. Configures the NTP version • <1-4> – Select the NTP version from 1 - 4.

```
ntp server <IP> {key <1-65534> md5 [0 <WORD>|2<WORD>|<WORD>]} {prefer version
<1-4>|
version <1-4>}
```

server <PEER-IP>	Configures a NTP server association
key <1-65534> md5 [0 <WORD>| 2 <WORD>|<WORD>]	Optional. Defines the authentication key for trusted time sources • <1-65534> – Specify the peer key number. • md5 – Sets MD5 authentication • 0 <WORD> – Configures a clear text password • 2 <WORD> – Configures an encrypted password • <WORD> – Sets an authentication key
prefer version <1-4>	Optional. Prefers this peer when possible • version – Optional. Configures the NTP version • <1-4> – Select the NTP version from 1 - 4.

```
ntp server <IP> {prefer version <1-4>|version <1-4> prefer}
```

server <PEER-IP>	Configures a NTP server association
prefer {version <1-4>}	Optional. Prefers this peer when possible • version – Optional. Configures the NTP version • <1-4> – Select the NTP version from 1 - 4.
version <1-4> prefer	Optional. Configures a NTP version as preferred • <1-4> – Select the NTP version from 1 - 4.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#ntp server 172.16.10.10

rfs7000-37FABE(config-profile-default-rfs7000)#ntp server 172.16.10.10
version 1 prefer

rfs7000-37FABE(config-profile-default-rfs7000)#show context
```

```
profile rfs7000 default-rfs7000
 mint link ip 1.2.3.4
 mint level 1 area-id 88
 bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
.........................................
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge3
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge4
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface pppoe1
 use firewall-policy default
 ntp server 172.16.10.10 prefer version 1
 misconfiguration-recovery-time 65
 noc update-interval 25
service pm sys-restart
 router ospf
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Disables or reverts settings to their default

power-config

Profile Config Commands

Configures the power option mode. Sets the amount of power that the access point draws.

Single radio model access points always operate using a full power configuration. The power management configurations described in this section do not apply to single radio models. When an access point is powered on for the first time, the system determines the power budget available to the access point. If 802.3af is selected, the access point assumes 12.95 watts is available. If the mode is changed, the access point requires a reset to implement the change. If 802.3at is selected, the access point assumes 23 - 26 watts is available.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

Syntax:

```
power-config [af-option|at-option|mode]

power-config [af-option|at-option] [range|throughput]

power-config mode [auto|3af]
```

Parameters

`power-config [af-option|at-option] [range|throughput]`

af-option [range|throughput]	Configures the 802.3.af power mode option. The options are: • range – Configures the af power range mode. This mode provides higher power but fewer transmission (tx) chains. Select range when range is preferred over performance for broadcast/multicast (group) traffic. The data rates used for range are the lowest defined basic rates. • throughput – Configures the af power throughput mode. This mode provides lower power but has more tx chains. This is the default setting. Select throughput to transmit packets at the radio's highest defined basic rate (based on the radio's current basic rate settings). This option is optimal in environments where transmission range is secondary to broadcast/multicast transmission performance.
at-option [range|throughput]	Configures the 802.3 at power mode option. The options are: • range – Configures the at power range mode. This mode provides higher power but fewer tx chains. Select range when range is preferred over performance for broadcast/multicast (group) traffic. The data rates used for range are the lowest defined basic rates. • throughput – Configures the at power throughput mode. This mode provides lower power but has more tx chains. This is the default setting. Select throughput to transmit packets at the radio's highest defined basic rate (based on the radio's current basic rate settings). This option is optimal in environments where transmission range is secondary to broadcast/multicast transmission performance.

`power-config mode [auto|3af]`

mode [auto|3af]	Configures the AP power mode • 3af – Forces an AP to power up in the 802.3af power mode • auto – Sets the detection auto mode (default setting) The automatic power-config mode enables an access point to automatically determine the best power configuration based on the available power budget.

Example

```
rfs7000-37FABE(config-profile-defalut-rfs7000)#power-config af-option range
% Warning: AP must be restarted for power-management change to take effect.
rfs7000-37FABE(config-profile-defalut-rfs7000)#

rfs7000-37FABE(config-profile-defalut-rfs7000)#power-config at-option
throughput
% Warning: AP must be restarted for power-management change to take effect.
rfs7000-37FABE(config-profile-defalut-rfs7000)#

rfs7000-37FABE(config-profile-default-rfs7000)#power-config af-option range
% Error on default-rfs7000: AP power configuration not available for rfs7000
platform
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Reverts the power mode setting on this profile to default

preferred-controller-group

Profile Config Commands

Specifies the controller group preferred for adoption

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
preferred-controller-group <WORD>
```

Parameters

```
preferred-controller-group <WORD>
```

<WORD>	Specify the name of the controller (wireless controller or service platform) group preferred for adoption. Devices using this profile are added, on adoption, to the controller group specified here.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#preferred-controller-group
testGroup

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 mint link ip 1.2.3.4
 mint level 1 area-id 88
 bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
.....................................................
 qos trust 802.1p
 interface pppoe1
 use firewall-policy default
 ntp server 172.16.10.10 prefer version 1
 preferred-controller-group testGroup
 misconfiguration-recovery-time 65
 noc update-interval 25
service pm sys-restart
 router ospf
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Removes the preferred controller group configuration

preferred-tunnel-controller

Profile Config Commands

Configures the tunnel controller's name preferred for tunneling extended VLAN traffic. Devices using this profile will prefer to route their extended VLAN traffic through the specified tunnel controller (wireless controller or service platform).

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
preferred-tunnel-controller <NAME>
```

Parameters

```
preferred-tunnel-controller <NAME>
```

preferred-tunnel-controller <NAME>	Configures the preferred tunnel name

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#preferred-tunnel-controller
testtunnel
```

Related Commands:

no	Removes the preferred tunnel configuration

radius

Profile Config Commands

Configures device level RADIUS authentication parameters

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
radius [nas-identifier|nas-port-id] <WORD>
```

Parameters

```
radius [nas-identifier|nas-port-id] <WORD>
```

nas-identifier <WORD>	Specifies the RADIUS *Network Access Server* (NAS) identifier attribute used by this device • <WORD> – Specifies the NAS identifier
nas-port-id <WORD>	Specifies the RADIUS NAS port ID attribute used by this device • <WORD> – Specifies the NAS port ID

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#radius nas-port-id 1

rfs7000-37FABE(config-profile-default-rfs7000)#radius nas-identifier test

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 mint link ip 1.2.3.4
 mint level 1 area-id 88
 bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
 radius nas-identifier test
 radius nas-port-id 1
 neighbor-info-interval 6
 neighbor-inactivity-timeout 500
--More--
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Disables or reverts settings to their default

rf-domain-manager

Profile Config Commands

Enables the RF Domain manager

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
rf-domain-manager [capable|priority <1-255>]
```

Parameters

```
rf-domain-manager [capable|priority <1-255>]
```

capable	Enables a device to become a site manager
priority <1-255>	Assigns a priority value for site manager selection • <1-255> – Select a priority value from 1 - 255.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#rf-domain-manager priority 9

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
```

```
 mint link ip 1.2.3.4
 mint level 1 area-id 88
 ........................................
 rf-domain-manager priority 9
 preferred-controller-group testGroup
 misconfiguration-recovery-time 65
 noc update-interval 25
service pm sys-restart
 preferred-tunnel-controller testtunnel
 router ospf
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Disables or reverts settings to their default

router

Profile Config Commands

Configures dynamic router protocol settings. For more details on router commands, see *ROUTER-MODE COMMANDS*.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
router ospf
```

Parameters

```
router ospf
```

ospf	Enables OSPF settings. Changes configuration mode to router mode OSPF is a link-state IGP. OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighbor routers and constructs a network topology. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#router ospf

rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#?
Router OSPF Mode commands:
  area                 OSPF area
  auto-cost            OSPF auto-cost
  default-information   Distribution of default information
  ip                   Internet Protocol (IP)
  network              OSPF network
  no                   Negate a command or set its defaults
```

```
  ospf                  Ospf
  passive               Make OSPF Interface as passive
  redistribute          Route types redistributed by OSPF
  route-limit           Limit for number of routes handled OSPF process
  router-id             Router ID
  vrrp-state-check      Publish interface via OSPF only if the interface VRRP
                        state is not BACKUP

  clrscr                Clears the display screen
  commit                Commit all changes made in this session
  do                    Run commands from Exec mode
  end                   End current mode and change to EXEC mode
  exit                  End current mode and down to previous mode
  help                  Description of the interactive help system
  revert                Revert changes
  service               Service Commands
  show                  Show running system information
  write                 Write running configuration to memory or terminal

rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#
```

Related Commands:

no	Disables OSPF settings

spanning-tree

Profile Config Commands

Enables spanning tree commands. Use these commands to configure the errdisable, multiple spanning tree and portfast settings.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
spanning-tree [errdisable|mst|portfast]

spanning-tree errdisable recovery [cause bpduguard|interval <10-1000000>]

spanning-tree mst
[<0-15>|cisco-interoperability|enable|forward-time|hello-time|
          instance|max-age|max-hops|region|revision]

spanning-tree mst [<0-15> priority <0-61440>|cisco-interoperability
[enable|disable]|
          enable|forward-time <4-30>|hello-time <1-10>|instance
<1-15>|max-age <6-40>|
          max-hops <7-127>|region <LINE>|revision <0-255>]
```

```
spanning-tree portfast [bpdufilter|bpduguard] default
```

Parameters

```
spanning-tree errdisable recovery [cause bpduguard|interval <10-1000000>]
```

errdisable	Disables or shutsdown ports where traffic is looping, or ports with traffic in one direction
recovery	Enables the timeout mechanism for a port to be recovered
cause bpduguard	Specifies the reason for errdisable • bpduguard – Recovers from errdisable due to bpduguard
interval <10-1000000>	Specifies the interval after which a port is enabled • <10-1000000> – Specify a value from 10 - 1000000 seconds.

```
spanning-tree mst [<0-15> priority <0-61440>|cisco-interoperability
[enable|disable]|
enable|forward-time <4-30>|hello-time <1-10>|instance <1-15>|max-age
<6-40>|max-hops
<7-127>|region <LINE>|revision <0-255>]
```

mst	Configures *Multiple Spanning Tree* (MST) commands
<0-15> priority <0-61440>	Specifies the number of instances required to configure MST. Select a value from 0 -15. • priority – Sets the bridge priority to the specified value. Use the no parameter with this command to restore the default bridge priority value. • <0-61440> – Sets the bridge priority in increments (Lower priority indicates greater likelihood of becoming root)
cisco interoperability [enable|disable]	Enables or disables CISCO interoperability
enable	Enables MST protocol
forward-time <4-30>	Specifies the forwarding delay time in seconds • <4-30> – Specify a value from 4 - 30 seconds.
hello-time <1-10>	Specifies the hello BDPU interval in seconds • <1-10> – Specify a value from 1 - 10 seconds.
instance <1-15>	Defines the instance ID to which the VLAN is associated • <1-15> – Specify an instance ID from 1 - 10.
max-age <6-40>	Defines the maximum time to listen for the root bridge • <6-40> – Specify a value from 4 - 60 seconds.
max-hops <7-127>	Defines the maximum hops when BPDU is valid • <7-127> – Specify a value from 7 - 127.
region <LINE>	Specifies the MST region • <LINE> – Specify the region name.
revision <0-255>	Sets the MST bridge revision number. This enables the retrieval of configuration information. • <0-255> – Specify a value from 0 - 255.

```
spanning-tree portfast [bpdufilter|bpduguard] default
```

portfast [bpdufilter| bpduguard] default	Enables PortFast on a bridge • bpdufilter default – Sets the BPDU filter for the port. Use the no parameter with this command to revert to default. The spanning tree protocol sends BPDUs from all ports. Enabling the BPDU filter ensures that PortFast enabled ports do not transmit or receive BPDUs • bpduguard default – Guards PortFast ports against BPDU receive • default – Enables the BPDU filter on PortFast enabled ports by default

Usage Guidelines:

If a bridge does not hear BPDUs from the root bridge within the specified interval, assume the network has changed and recomputed the spanning-tree topology.

Generally, spanning tree configuration settings in the config mode define the configuration for bridge and bridge instances.

MSTP is based on instances. An instance is a group of VLANs with a common spanning tree. A single VLAN cannot be associated with multiple instances.

Wireless Controllers or service platforms with the same instance, VLAN mapping, revision number and region names define a unique region. Wireless Controllers or service platforms in the same region exchange BPDUs with instance record information within.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#spanning-tree errdisable
recovery cause bpduguard

rfs7000-37FABE(config-profile-default-rfs7000)#spanning-tree mst 2 priority
4096

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 mint link ip 1.2.3.4
 mint level 1 area-id 88
 bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
 radius nas-identifier test
 radius nas-port-id 1
 neighbor-info-interval 6
 neighbor-inactivity-timeout 500
 spanning-tree mst 2 priority 4096
 spanning-tree errdisable recovery cause bpduguard
 autoinstall configuration
--More--
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Disables or reverts settings to their default

tunnel-controller

Profile Config Commands

Configures the tunneled WLAN (extended VLAN) wireless controller or service platform's name

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
tunnel-controller <NAME>
```

Parameters

```
tunnel-controller <NAME>
```

tunnel-controller <NAME>	Configures the tunneled WLAN (extended VLAN) wireless controller or service platform's name • <NAME> – Specify a name.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#tunnel-controller testgroup
```

Related Commands:

no	Removes the configured the tunneled WLAN (extended VLAN) wireless controller or service platform's name

use

Profile Config Commands

Associates existing policies with this profile

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax: Profiles Mode

```
use [advanced-wips-policy|auto-provisioning-policy|captive-portal|

client-identity-group|dhcp-server-policy|event-system-policy|firewall-policy|

global-assoc-policy|management-policy|radius-server-policy|role-policy|
          routing-policy|critical-resource-policy]
```

Syntax: Device Mode

```
use [advanced-wips-policy|auto-provisioning-policy|captive-portal|

client-identity-group|dhcp-server-policy|event-system-policy|firewall-policy|

global-assoc-list|management-policy|profile|radius-server-policy|rf-domain|

role-policy|routing-policy|wips-policy|critical-resource-policy|smart-rf-poli
cy|
          trustpoint]
```

NOTE
The following tables contain the 'use' command parameters for the Profile and Device configuration modes.

ParametersProfiles Mode

```
use
[advanced-wips-policy|auto-provisioning-policy|captive-portal|client-identity
-group|dhcp-server-policy|event-system-policy|firewall-policy|global-assoc-li
st|
management-policy|radius-server-policy|role-policy|routing-policy|critical-re
source-policy]
```

use	Associates the specified policies with this profile The specified policies should be existing and configured.
advanced-wips-policy <POLICY-NAME>	Associates an advanced WIPS policy • <POLICY-NAME> – Specify the WIPS policy name.
auto-provisioning-policy <POLICY-NAME>	Associates an auto provisioning policy • <POLICY-NAME> – Specify the auto provisioning policy name.
captive-portal server <CAPTIVE-PORTAL>	Configures access to a specified captive portal with this profile • <CAPTIVE-PORTAL> – Specify the captive portal name.
client-identity <CLIENT-IDENTITY-GROUP-NAME>	Associates an existing client identity group with this profile • <CLIENT-IDENTITY-GROUP-NAME> – Specify the client identity group name. For more information on the 'client-identity' and 'client-identity-group' commands, see *client-identity* and *client-identity-group*.
dhcp-server-policy <DHCP-POLICY>	Associates a DHCP server policy • <DHCP-PLOICY> – Specify the DHCP server policy name.
event-system-policy <EVENT-SYSTEM-POLICY>	Associates an event system policy • <EVENT-SYSTEM-POLICY> – Specify the event system policy name.
firewall-policy <FW-POLICY>	Associates a firewall policy • <FW-POLICY> – Specify the firewall policy name.
global-assoc-list server <GLOBAL-ASSOC-LIST-NAME>	Associates the specified global association list with the controller profile • <GLOBAL-ASSOC-LIST-NAME> – Specify the global association list name. Once associated, the controller, using this profile, applies this association list to requests received from all adopted APs. For more information on global association list, see *global-association-list*.
management-policy <MNGT-POLICY>	Associates a management policy • <MNGT-POLICY> – Specify the management policy name.
radius-server-policy <RADIUS-POLICY>	Associates a device onboard RADIUS policy • <RADIUS-POLICY> – Specify the RADIUS policy name.

role-policy <ROLE-POLICY>	Associates a role policy • <ROLE-POLICY> – Specify the role policy name.
routing-policy <ROUTING-POLICY>	Associates a routing policy • <ROUTING-POLICY> – Specify the routing policy name.

Parameters Device Mode

```
use [advanced-wips-policy|auto-provisioning-policy|captive-portal|
client-identity-group|dhcp-server-policy|event-system-policy|firewall-policy|
management-policy|profile|radius-server-policy|rf-domain|role-policy|routing-
policy|
wips-policy|critical-resource-policy|smart-rf-policy|trustpoint]
```

use	Associates the following policies with this device:
advanced-wips-policy <POLICY-NAME>	Associates an advanced WIPS policy • <POLICY-NAME> – Specify the advanced WIPS policy name.
auto-provisioning-policy <POLICY-NAME>	Associates an auto provisioning policy • <POLICY-NAME> – Specify the auto provisioning policy name.
captive-portal server <CAPTIVE-PORTAL>	Configures access to a specified captive portal • <CAPTIVE-PORTAL> – Specify the captive portal name.
client-identity <CLIENT-IDENTITY-GROUP-NAME>	Associates an existing client identity group with this device • <CLIENT-IDENTITY-GROUP-NAME> – Specify the client identity group name. For more information on the 'client-identity' and 'client-identity-group' commands, see *client-identity* and *client-identity-group*.
dhcp-server-policy <DHCP-POLICY>	Associates a DHCP server policy • <DHCP-PLOICY> – Specify the DHCP server policy name.
event-system-policy <EVENT-SYSTEM-POLICY>	Associates an event system policy • <EVENT-SYSTEM-POLICY> – Specify the event system policy name.
firewall-policy <FW-POLICY>	Associates a firewall policy • <FW-POLICY> – Specify the firewall policy name.
global-assoc-list server <GLOBAL-ASSOC-LIST-NAME>	Associates the specified global association list with the device (controller) • <GLOBAL-ASSOC-LIST-NAME> – Specify the global association list name. Once associated, the controller applies this association list to requests received from all adopted APs. For more information on global assoc it ion list, see *global-association-list*.
igmp-snoop-policy <IGMP-POLICY>	Associates an IGMP snoop policy • <IGMP-POLICY> – Specify the IGMP snoop policy name.
management-policy <MNGT-POLICY>	Associates a management policy • <MNGT-POLICY> – Specify the management policy name.
profile <PROFILE-NAME>	Associates a profile with this device • <PROFILE-NAME> – Specify the profile name.
radius-server-policy <RADIUS-POLICY>	Associates a device onboard RADIUS policy • <RADIUS-POLICY> – Specify the RADIUS policy name.
rf-domain <RF-DOMAIN-NAME>	Associates an RF Domain • <RF-DOMAIN-NAME> – Specify the RF Domain name.
role-policy <ROLE-POLICY>	Associates a role policy • <ROLE-POLICY> – Specify the role policy name.
routing-policy <ROUTING-POLICY>	Associates a routing policy • <ROUTING-POLICY> – Specify the routing policy name.

wips-policy <WIPS-POLICY>	Associates a WIPS policy • <WIPS-POLICY> – Specify the WIPS policy name.
critical-resource-policy <CRT-RESOURCE-POLICY>	Associates a critical resource monitoring policy • <CRT-RESOURCE-POLICY> – Specify the critical resource policy name.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#use advanced-wips-policy
TestWIPSPolicy

rfs7000-37FABE(config-profile-default-rfs7000)#use event-system-policy
TestEventSysPolicy

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 mint link ip 1.2.3.4
 mint level 1 area-id 88
 ................................................
 interface ge3
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge4
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface pppoe1
 use event-system-policy TestEventSysPolicy
 use firewall-policy default
 ntp server 172.16.10.10 prefer version 1
--More--
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Disassociates a specified policy from this profile

vrrp

Profile Config Commands

Configures VRRP group settings

A default gateway is a critical resource for connectivity. However, it is prone to a single point of failure. Thus, redundancy for the default gateway is required. If WAN backhaul is available, and a router failure occurs, then the controller should act as a router and forward traffic on to its WAN link.

Define an external VRRP configuration when router redundancy is required in a network requiring high availability.

Central to VRRP configuration is the election of a VRRP master. A VRRP master (once elected) performs the following functions:

- Responds to ARP requests
- Forwards packets with a destination link layer MAC address equal to the virtual router's MAC address

- Rejects packets addressed to the IP address associated with the virtual router, if it is not the IP address owner
- Accepts packets addressed to the IP address associated with the virtual router, if it is the IP address owner or accept mode is true.

The nodes that lose the election process enter a backup state. In the backup state they monitor the master for any failures, and in case of a failure one of the backups, in turn, becomes the master and assumes the management of the designated virtual IPs. A backup does not respond to an ARP request, and discards packets destined for a virtual IP resource.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
vrrp [<1-255>|version]

vrrp <1-255>
[delta-priority|description|interface|ip|monitor|preempt|priority|
          sync-group|timers]

vrrp <1-255> [delta-priority <1-253>|description <LINE>|ip <IP> {<IP>}|
          preempt {delay <1-65535>}|priority <1-254>|sync-group]

vrrp <1-255> interface [<INTERFACE-NAME>|ge <1-4>|me1|port-channel
<1-2>|pppoe1|
          vlan <1-4094>|wwan1]

vrrp <1-255> monitor [<IF-NAME>|critical-resource|pppoe1|vlan|wwan1]
vrrp <1-255> monitor [<IF-NAME>|pppoe1|vlan <1-4094>|wwan1] {(<IF-NAME>|
          critical-resource|pppoel|vlan|wwan1)}
vrrp <1-255> monitor critical-resource <CRM-NAME1> <CRM-NAME2> <CRM-NAME3>
<CRM-NAME4>
          (action [decrement-priority|increment-priority]
{<IF-NAME>|pppoe1|vlan|wwan1})

vrrp <1-255> timers advertise [<1-255>|centiseconds <25-4095>|msec <250-999>]

vrrp version [2|3]
```

Parameters

```
vrrp <1-255> [delta-priority <1-253>|description <LINE>|vrrp ip <IP> {<IP>}|
preempt {delay <1-65535>}|priority <1-254>|sync-group]
```

vrrp <1-255>	Configures the virtual router ID from 1- 255. Identifies the virtual router the packet is reporting status for
delta-priority <1-253>	Configures the priority to decrement (local link monitoring and critical resource monitoring) or increment (critical resource monitoring) • <1-253> – Specify the delta priority level from 1- 253.

description <LINE>	Configures a text description for the virtual router to further distinguish it from other routers with similar configuration • <LINE> – Provide a description (a string from 1- 64 characters in length)
ip <IP-ADDRESSES>	Identifies the IP address(es) backed by the virtual router. These are IP addresses of Ethernet switches, routers, and security appliances defined as virtual router resources. • <IP-ADDRESSES> – Specify the IP address(es) in the A.B.C.D format. This configuration triggers VRRP operation.
preempt {delay <1-65535>}	Controls whether a high priority backup router preempts a lower priority master. This field determines if a node with higher priority can takeover all virtual IPs from a node with lower priority. This feature is enabled by default. • delay – Optional. Configures the pre-emption delay timer from 1 - 65535 seconds (default is 0 seconds). This option can be used to delay sending out the master advertisement or, in case of monitored link coming up, adjusting the VRRP priority by priority delta.
priority <1-254>	Configures the priority level of the router within a VRRP group. This value determines which node is elected as the Master. Higher values imply higher priority, value 254 has the highest precedence (default is 100).
sync-group	Adds this VRRP group to a synchronized group. To trigger VRRP failover, it is essential all individual groups within a synchronized group have failover. VRRP failover is triggered if an advertisement is not received from the virtual masters that are part of this VRRP sync group. This feature is disabled by default.

```
vrrp <1-255> interface [<INTERFACE-NAME>|ge <1-4>|me1|port-channel
<1-2>|pppoe1|
vlan <1-4094>|wwan1]
```

vrrp <1-255>	Configures the virtual router ID from 1- 255. Identifies the virtual router the packet is reporting status for.
interface [<INTERFACE-NAME>| ge <1-4>|me1| port-channel <1-2>| pppoe1|vlan <1-4094>| wwan1]	Enables VRRP on the selected SVI interface • <INTERFACE-NAME> – Enables VRRP on the VLAN interface specified by the <INTERFACE-NAME> parameter • ge <1-4> – Enables VRRP on the specified GigabitEthernet interface • me1 – Enables VRRP on the FastEthernet interface • pppoe1 – Enables VRRP on the PPP over Ethernet interface • port-channel <1-2> – Enables VRRP on the port channel interface • vlan <1-4094> – Enables VRRP on the specified VLAN interface • wwan1 – Enables VRRP on the Wireless WAN interface

```
vrrp <1-255> monitor critical-resource <CRM-NAME1> <CRM-NAME2> <CRM-NAME3>
<CRM-NAME4> (action [decrement-priority|increment-priority]
{<IF-NAME>|pppoe1|vlan|wwan1})
```

vrrp <1-255>	Configures the virtual router ID from 1- 255. Identifies the virtual router the packet is reporting status for.
monitor	Enables link monitoring or *Critical Resource Monitoring* (CRM)
critical-resource <CRM-NAME1>	Specifies the name of the critical resource to monitor. VRRP can be configured to monitor maximum of four critical resources. Use the <CRM-NAME2>, <CRM-NAME3>, and <CRM-NAME4> to provide names of the remaining three critical resources. By default VRRP is configured to monitor all critical resources on the device.
action [decrement-priority| increment-priority]	Sets the action on critical resource down event. It is a recursive parameter that sets the action for each of the four critical resources being monitored. • decrement-priority – Decrements the priority of virtual router on critical resource down event • increment-priority – Increments the priority of virtual router on critical resource down event
<IF-NAME>	Optional. Enables interface monitoring • <IF-NAME> – Specify the interface name to monitor
pppoe1	Optional. Enables *Point-to-Point Protocol* (PPP) over Ethernet interface monitoring

vlan <1-4094>	Optional. Enables VLAN (switched virtual interface) interface monitoring • <1-4094> – Specify the VLAN interface ID from 1- 4094.
wwan1	Optional. Enables Wireless WAN interface monitoring

```
vrrp <1-255> timers advertise [<1-255>|centiseconds <25-4095>|msec <250-999>]
```

vrrp <1-255>	Configures the virtual router ID from 1- 255. Identifies the virtual router the packet is reporting status for.
timers	Configures the timer that runs every interval
advertise [<1-255>| centiseconds <25-4095>| msec <250-999>]	Configures the VRRP advertisements time interval. This is the interval a master sends out advertisements on each of its configured VLANs. • <1-255> – Configures the timer interval from 1- 255 seconds. (applicable for VRRP version 2 only) • centiseconds <25-4095> – Configures the timer interval in centiseconds (1/100th of a second). Specify a value between 25 - 4095 centiseconds (applicable for VRRP version 3 only) • msec <250-999> – Configures the timer interval in milliseconds (1/1000th of a second). Specify a value between 250 - 999 msec (applicable for VRRP version 2 only) Default is 1 second.

```
vrrp version [2|3]
```

vrrp version [2|3]	Configures one of the following VRRP versions: • 2 – VRRP version 2 (RFC 3768) • 3 – VRRP version 3 (RFC 5798 only IPV4) (default setting) The VRRP version determines the router redundancy. Version 3 supports sub-second (centisecond) VRRP failover and support services over virtual IP.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#vrrp version 3

rfs7000-37FABE(config-profile-default-rfs7000)#vrrp 1 sync-group

rfs7000-37FABE(config-profile-default-rfs7000)#vrrp 1 delta-priority 100

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 bridge vlan 1
 ..................................................
 vrrp 1 timers advertise 1
 vrrp 1 preempt
 vrrp 1 sync-group
 vrrp 1 delta-priority 100
 vrrp version 3
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Reverts VRRP settings

wep-shared-key-auth

Profile Config Commands

Enables support for 802.11 WEP shared key authentication

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
wep-shared-key-auth
```

Parameters

None

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#wep-shared-key-auth

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
 wep-shared-key-auth
 autoinstall configuration
 autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 interface me1
 interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge2
  ip dhcp trust
--More--
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Disable support for 802.11 WEP shared key authentication

service

Profile Config Commands

Service commands are used to view and manage configurations. The service commands and their corresponding parameters vary from mode to mode.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
service
[critical-resource|fast-switching|enable|global-association-list|meshpoint|
          pm|power-config|radius|rss-timeout|watchdog|wireless|show]

service critical-resource port-mode-source-ip <IP>

service enable [l2tpv3|pppoe|adiusd]

service global-association-list blacklist-interval <1-65535>

service meshpoint loop-prevention-port [<L2-INTERFACE-NAME>|ge <1-5>|
          port-channel <1-2>|up1]

service pm sys-restart

service power-config [3af-out|force-3at]

service radius dynamic-authorization additional-port <1-65535>

service rss-timeout <0-86400>

service watchdog

service wireless [br650|client|cred-cache-sync|test|wispe-controller-port]

service wireless br650 legacy-auto-update-image <FILE>
service wirless client tx-deauth on-radar-detect
service wireless cred-cache-sync [full|interval <30-864000>|never|partial]
service wireless test [max-rate|max-retries|min-rate]
service wireless test [max-rate|min-rate]
[1,2,5.5,6,11,12,18,24,36,48,54,mcs0,
          mcs1,.....mcs23]
service wireless test max-retries <0-15>
service wireless wispe-controller-port <1-65535>

service show cli
```

Parameters

```
service critical-resource port-mode-source-ip <IP>
```

critical-resource port-mode-source-ip <IP>	Hard codes a source IP for critical resource management

	`service enable [l2tpv3|pppoe|radiusd]`
service enable l2tpv3	Enables/disables L2TPv3 on this profile This feature is not supported on Brocade Mobility 650 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point, Brocade Mobility RFS4000, Brocade Mobility RFS6000, and Brocade Mobility RFS7000. It is supported only on Brocade Mobility 6511 Access Point.
service enable pppoe	Enables PPPoE features. When executed on a device, enables PPPoE on the logged device. When excuted on a profile, enables PPPoE on all devices using that profile.
service enable radiusd	Enables RADIUSD features. When executed on a device, enables RADIUSD on the logged device. When excuted on a profile, enables RADIUSD on all devices using that profile.

	`service global-association-list blacklist-interval <1-65535>`
service global-association-list	Configures global association list related parameters
blacklist-interval <1-65535>	Configures the period for which a client is blacklisted. A client is considered blacklisted after being denied access by the server. • <1-65535> – Specify a value from 1 -65535 seconds.

	`service meshpoint loop-prevention-port [<L2-INTERFACE-NAME>|ge <1-4>| port-channel <1-2>]`
meshpoint loop-prevention-port	Limits meshpoint loop prevention to a single port
<L2-INTERFACE-NAME>	Limits meshpoint loop prevention on a specified Ethernet interface • <L2-INTERFACE-NAME> – Specify the layer 2 Ethernet interface name.
ge <1-4>	Limits meshpoint loop prevention on a specified GigabitEthernet interface • ge <1-4> – Specify the GigabitEthernet interface index from 1 - 4.
port-channel <1-2>	Limits meshpoint loop prevention on a specified port-channel interface • port-channel <1-2> – Specify the port-channel interface index from 1 - 2.

	`service pm sys-restart`
pm sys-restart	Enables the *process monitor* (PM) to restart the system when a process fails

	`service power-config [3af-out|force-3at]`
power-config 3af-out	Enables LLDP power negotiation, but uses 3af power
power-config force-3at	Disables LLDP negotiation and force 802.3at power configuration

	`service radius dynamic-authorization additional-port <1-65535>`
radius dynamic-authorization additional-port <1-65535>	Configures an additional UDP port used by the device to listen for dynamic authorization messages • <1-65535> – Specify a value from 1 - 65535. The Cisco *Identity Services Engine* (ISE) server uses port 1700.

	`service rss-timeout <0-86400>`
rss-timeout <0-86400>	Configures the duration, in seconds, for which an adopted access point will continue to provide wireless functions even after loosing controller adoption. • <0-86400> – Specify a value from 0 - 86400 seconds.

	`service watchdog`
watchdog	Enables/disables the watchdog. This feature is enabled by default. Enabling the watchdog option implements heartbeat messages to ensure other associated devices are up and running and capable of effectively inter-operating with the controller.
	`service wireless br650 legacy-auto-update-image <FILE>`
wireless br650	Invokes Brocade Mobility 650 Access Point related service commands
legacy-auto-update-image <FILE>	Configures the Brocade Mobility 650 Access Point image file details, such as location and file name • <FILE> – Provides the path and name of the Brocade Mobility 650 Access Point image file (for example, flash:/br.img)
	`service wireless client tx-deauth on-radar-detection`
wireless client	Configures wireless client and stations related settings
tx-deauth on-radar-detection	Enables/disables access points to transmit deauth to clients when changing channels on radar detection
	`service wireless cred-cache-sync [full|interval <30-864000>|never|partial]`
wireless cred-cache-sync	Configures the credential cache's synchronization parameters. The parameters are: full, interval, never, and partial.
full	Enables synchronization of all credential cache entries
interval <30-864000>	Sets the interval, in seconds, at which the credential cache is synchronized • <30-864000> – Specify a value from 30 - 864000 seconds.
partial	Enables partial synchronization of parameters for associated clients, with credential cache close to aging out
	`service wireless test [max-rate|min-rate] [1,2,5.5,6,11,12,18,24, 36,48,54,mcs0, mcs1,.....mcs23]`
wireless test	Configures the serviceability parameters used for testing
[max-rate|min-rate]	Configures the maximum and minimum data rates for clients using rate-scaling
[1,2,5.5,.mcs23]	Select the maximum and minimum data rates applicable.
	`service wireless test max-retries <0-15>`
wireless test	Configures the serviceability parameters used for testing
max-retries <0-15>	Configures the maximum number of retries per packet
	`service wireless wispe-controller-port <1-65535>`
wispe-controller-port <1-65535>	Resets the *WIreless Switch Protocol Enhanced* (WISPe) controller port. This is the UDP port used to listen for WISPe. • <1-65535> – Specify a value from 1 -65535.
	`service show cli`
show cli	Displays running system configuration details • cli – Displays the CLI tree of the current mode
	`service fast-switching`
fast-switching	Enables fast switching of packets in the hardware Use the *no* > *service* > *fast-switching* to disable this feature.

Example

```
rfs7000-37FABE(config-profile-testrfs71xx)#service radius
dynamic-authorization additional-port 1700
rfs7000-37FABE(config-profile-testrfs71xx)#

rfs7000-37FABE(config-profile-testrfs71xx)#show context
profile rfs7000 test
 service radius dynamic-authorization additional-port 1700
 no autoinstall configuration
 no autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
--More--
rfs7000-37FABE(config-profile-testrfs71xx)#
```

Related Commands:

no	Removes or resets service command parameters

Device Config Commands

PROFILES

Use the (config) instance to configure device specific parameters

To navigate to this instance, use the following commands:

```
<DEVICE>(config)#<DEVICE-TYPE> <MAC>
<DEVICE>(config-device-<MAC>)#?
Device Mode commands:
  adopter-auto-provisioning-policy-lookup  Use centralized auto-provisioning
                                           policy when adopted by another
                                           controller
  adoption-site                            Set system's adoption site
  alias                                    Alias
area                                      Set name of area where the system
                                           is located
  arp                                      Address Resolution Protocol (ARP)
  auto-learn-staging-config                Enable learning network
                                           configuration of the devices that
                                           come for adoption
  autogen-uniqueid                         Autogenerate a unique id
  autoinstall                              Autoinstall settings
  bridge                                   Ethernet bridge
  captive-portal                           Captive portal
  cdp                                      Cisco Discovery Protocol
  channel-list                             Configure channel list to be
                                           advertised to wireless clients
  cluster                                  Cluster configuration
  configuration-persistence                Enable persistence of configuration
                                           across reloads (startup config
                                           file)
  contact                                  Configure the contact
```

```
controller                          WLAN controller configuration
country-code                        Configure the country of operation
critical-resource                   Critical Resource
crypto                              Encryption related commands
device-upgrade                      Device firmware upgrade
dot1x                               802.1X
dscp-mapping                        Configure IP DSCP to 802.1p
                                    priority mapping for untagged
                                    frames
email-notification                  Email notification configuration
enforce-version                     Check the firmware versions of
                                    devices before interoperating
environmental-sensor                Environmental Sensors Configuration
events                              System event messages
export                              Export a file
floor                               Set the floor within a area where
                                    the system is located
geo-coordinates                     Configure geo coordinates for this
                                    device
gre                                 GRE protocol
hostname                            Set system's network name
http-analyze                        Specify HTTP-Analysis configuration
interface                           Select an interface to configure
ip                                  Internet Protocol (IP)
l2tpv3                              L2tpv3 protocol
l3e-lite-table                      L3e lite Table
layout-coordinates                  Configure layout coordinates for
                                    this device
led                                 Turn LEDs on/off on the device
led-timeout                         Configure the time for the led to
                                    turn off after the last radio state
                                    change
legacy-auto-downgrade               Enable device firmware to auto
                                    downgrade when other legacy devices
                                    are detected
legacy-auto-update                  Auto upgrade of legacy devices
license                             License management command
lldp                                Link Layer Discovery Protocol
load-balancing                      Configure load balancing parameter
location                            Configure the location
logging                             Modify message logging facilities
mac-address-table                   MAC Address Table
mac-auth                            802.1X
mac-name                            Configure MAC address to name
                                    mappings
memory-profile                      Memory profile to be used on the
                                    device
meshpoint-device                    Configure meshpoint device
                                    parameters
meshpoint-monitor-interval          Configure meshpoint monitoring
                                    interval
min-misconfiguration-recovery-time  Check controller connectivity after
                                    configuration is received
mint                                MiNT protocol
mirror                              Mirroring
misconfiguration-recovery-time      Check controller connectivity after
                                    configuration is received
neighbor-inactivity-timeout         Configure neighbor inactivity
                                    timeout
neighbor-info-interval              Configure neighbor information
```

```
                                        exchange interval
  no                                    Negate a command or set its
                                        defaults
  noc                                   Configure the noc related setting
  ntp                                   Ntp server A.B.C.D
  override-wlan                         Configure RF Domain level overrides
                                        for wlan
  power-config                          Configure power mode
  preferred-controller-group            Controller group this system will
                                        prefer for adoption
  preferred-tunnel-controller           Tunnel Controller Name this system
                                        will prefer for tunneling extended
                                        vlan traffic
  radius                                Configure device-level radius
                                        authentication parameters
  raid                                  RAID
  remove-override                       Remove configuration item override
                                        from the device (so profile value
                                        takes effect)
  rf-domain-manager                     RF Domain Manager
  router                                Dynamic routing
  rsa-key                               Assign a RSA key to a service
  sensor-server                         Motorola AirDefense sensor server
                                        configuration
  slot                                  PCI expansion Slot
  spanning-tree                         Spanning tree
  stats                                 Configure the stats related setting
  timezone                              Configure the timezone
  trustpoint                            Assign a trustpoint to a service
  tunnel-controller                     Tunnel Controller group this
                                        controller belongs to
  use                                   Set setting to use
  vrrp                                  VRRP configuration
  wep-shared-key-auth                   Enable support for 802.11 WEP
                                        shared key authentication

  clrscr                                Clears the display screen
  commit                                Commit all changes made in this
                                        session
  do                                    Run commands from Exec mode
  end                                   End current mode and change to EXEC
                                        mode
  exit                                  End current mode and down to
                                        previous mode
  help                                  Description of the interactive help
                                        system
  revert                                Revert changes
  service                               Service Commands
  show                                  Show running system information
  write                                 Write running configuration to
                                        memory or terminal

<DEVICE>(config-device-<MAC>)#
```

The following table summarizes device configuration mode commands.

Command	Description	Reference
adopter-auto-provisioning-policy-lookup	Enables the use of a centralized auto provisioning policy on this device	page 545
adoption-site	Sets the device's adoption site name	page 808
alias	Configures network, VLAN, and service aliases on a device	page 546
area	Sets the name of area where the system is deployed	*page 7-809*
arp	Configures ARP parameters	*page 7-552*
auto-learn-staging-config	Enables the automatic recognition of devices pending adoption	*page 7-553*
autogen-uniqueid	When executed in the device configuration mode, this command generates a unique ID for the logged device.	page 554
autoinstall	Autoinstalls firmware image and configuration setup parameters	*page 7-556*
bridge	Configures Ethernet Bridging parameters	*page 7-557*
captive-portal	Configures captive portal advanced Web page upload on this profile	page 572
cdp	Operates CDP on the device	*page 7-573*
channel-list	Configures channel list advertised to wireless clients	*page 7-810*
cluster	Sets cluster configuration	*page 7-574*
configuration-persistence	Enables configuration persistence across reloads	*page 7-576*
contact	Sets contact information	*page 7-810*
controller	Configures a WLAN's wireless controller or service platform	*page 7-577*
country-code	Configures wireless controller or service platform's country code	*page 7-811*
critical-resource	Monitors user configured IP addresses and logs their status	page 580
crypto	Configures data encryption protocols and settings	*page 7-583*
device-upgrade	Configures device firmware upgrade settings on this device	page 631
dot1x	Configures 802.1x standard authentication controls	page 634
dscp-mapping	Configures IP *Differentiated Services Code Point* (DSCP) to 802.1p priority mapping for untagged frames	*page 7-635*
email-notification	Configures e-mail notification	*page 7-636*
enforce-version	Checks the device firmware version before attempting connection	*page 7-638*
environmental-sensor	Configures the environmental sensor device settings. If the device is an environmental sensor, use this command to configures its settings,	page 639
events	Displays system event messages	*page 7-641*
export	Enables export of startup.log file after every boot	page 642
floor	Sets the building floor where the system is deployed	*page 7-812*
geo-coordinates	Configures the geographic coordinates for this device	page 813
gre	Enables GRE tunneling on this device	page 644
hostname	Sets a system's network name	*page 7-814*
http-analyze	Enables HTTP analysis on this device	page 652

Command	Description	Reference
interface	Selects an interface to configure	*page 7-653*
ip	Configures IP components	*page 7-744*
l2tpv3	Defines the *Layer 2 Tunnel Protocol* (L2TP) protocol for tunneling Layer 2 payloads using *Virtual Private Networks* (VPNs)	page 752
l3e-lite-table	Configures L3e Lite Table with this profile	page 753
layout-coordinates	Configures layout coordinates	*page 7-815*
led	Turns LEDs on or off	*page 7-754*
led-timeout	Configures the LED-timeout timer in the device or profile configuration mode	page 755
legacy-auto-downgrade	Enables legacy device firmware to auto downgrade	*page 7-756*
legacy-auto-update	Auto updates Brocade Mobility 650 Access Point and Brocade Mobility 71XX Access Point legacy device firmware	*page 7-757*
license	Adds a license for a device's features	page 815
lldp	Configures *Link Layer Discovery Protocol* (LLDP) settings for this profile	*page 7-757*
load-balancing	Configures load balancing parameters.	*page 7-759*
location	Configures the location the system is deployed	*page 7-817*
logging	Enables message logging	*page 7-763*
mac-address-table	Configures the MAC address table	*page 7-764*
mac-auth	Enables 802.1x authentication of hosts on this device	page 766
mac-name	Configures MAC name to name mappings	*page 7-818*
memory-profile	Configures memory profile used on the device	page 769
meshpoint-device	Configures meshpoint device parameters	page 769
meshpoint-monitor-interval	Configures meshpoint monitoring interval	page 770
min-misconfiguration-recovery-time	Configures the minimum device connectivity verification time	page 771
mint	Configures MiNT protocol commands	*page 7-772*
misconfiguration-recovery-time	Verifies device connectivity after a configuration is received	*page 7-775*
neighbor-inactivity-timeout	Configures a neighbor inactivity timeout	*page 7-776*
neighbor-info-interval	Configures the neighbor information exchange interval	*page 7-819*
no	Negates a command or resets values to their default settings	page 820
noc	Configures NOC settings	*page 7-780*
ntp	Configure the NTP server settings	*page 7-781*
override-wlan	Configures WLAN RF Domain level overrides	*page 7-823*
power-config	Configures power mode features	*page 7-783*
preferred-controller-group	Specifies the wireless controller or service platform group the system prefers for adoption	*page 7-784*

Command	Description	Reference
preferred-tunnel-controller	Configures the tunnel wireless controller or service platform preferred by the system for tunneling extended VLAN traffic	page 785
radius	Configures device-level RADIUS authentication parameters	*page 7-786*
remove-override	Removes device overrides	*page 7-824*
rf-domain-manager	Enables the RF Domain manager	*page 7-787*
router	Configures dynamic router protocol settings.	page 788
rsa-key	Assigns a RSA key to SSH	*page 7-826*
sensor-server	Configures an AirDefense sensor server	*page 7-827*
spanning-tree	Enables spanning tree commands	*page 7-789*
timezone	Configures wireless controller or service platform's time zone settings	*page 7-828*
trustpoint	Assigns a trustpoint to a service	*page 7-829*
tunnel-controller	Configures the tunneled WLAN (extended VLAN) wireless controller or service platform's name	page 791
use	Defines the settings used with this command	*page 7-792*
vrrp	Configures VRRP group settings	page 795
wep-shared-key-auth	Enables support for 802.11 WEP shared key authentication	*page 7-798*
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 799
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

adoption-site

Device Config Commands

Sets the device's adoption site name

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
adoption-site <SITE-NAME>
```

Parameters

```
adoption-site <SITE-NAME>
```

adoption-site <SITE-NAME>	Sets the device's adoption site name

Example

```
rfs4000-229D58(config-device-00-23-68-22-9D-58)#adoption-site MotoEcoSpace3B
rfs4000-229D58(config-device-00-23-68-22-9D-58)#
```

Related Commands:

no	Disables or reverts settings to their default

area

Device Config Commands

Sets the area where the system is deployed

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
area <AREA-NAME>
```

Parameters

```
area <AREA-NAME>
```

area <AREA-NAME>	Sets the area where the system is deployed <AREA-NAME> – Specify the area name.

Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#area RMZEcoSpace

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
br71xx 00-04-96-4A-A7-08
 use profile default-br71xx
 use rf-domain default
 hostname br7131-4AA708
 area RMZEcospace
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

Related Commands:

no	Disables or reverts settings to their default

channel-list

Device Config Commands

Configures the channel list advertised to wireless clients

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
channel-list [2.4GHz|5GHz|dynamic]
channel-list [2.4GHz <CHANNEL-LIST>|5GHz <CHANNEL-LIST>|dynamic]
```

Parameters

```
channel-list [2.4GHz <CHANNEL-LIST>|5GHz <CHANNEL-LIST>|dynamic]
```

2.4GHz <CHANNEL-LIST>	Configures the channel list advertised by radios operating in 2.4 GHz • <CHANNEL-LIST> – Specify a list of channels separated by commas or hyphens.
5GHz <CHANNEL-LIST>	Configures the channel list advertised by radios operating in 5.0 GHz • <CHANNEL-LIST> – Specify a list of channels separated by commas or hyphens.
dynamic	Enables dynamic (neighboring access point based) update of configured channel list

Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#channel-list 2.4GHz 1,2

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
br71xx 00-04-96-4A-A7-08
 use profile default-br71xx
 use rf-domain default
 hostname br7131-4AA708
 area RMZEcospace
 channel-list 2.4GHz 1,2
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

Related Commands:

no	Resets the channel list configuration

contact

Device Config Commands

Defines an administrative contact for a deployed device

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
contact <WORD>
```

Parameters

```
contact <WORD>
```

contact <WORD>	Specify the administrative contact name

Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#contact motorolasolutions

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
br71xx 00-04-96-4A-A7-08
 use profile default-br71xx
 use rf-domain default
 hostname br7131-4AA708
 area RMZEcospace
 contact motorolasolutions
 channel-list 2.4GHz 1,2
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

Related Commands:

no	Resets the administrative contact name

country-code

Device Config Commands

Defines the two digit country code for legal device deployment

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
country-code <WORD>
```

Parameters

```
country-code <COUNTRY-CODE>
```

country-code <COUNTRY-CODE>	Defines the two digit country code for legal device deployment • <COUNTRY-CODE> – Specify the two letter ISO-3166 country code.

Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#country-code us

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
br71xx 00-04-96-4A-A7-08
 use profile default-br71xx
 use rf-domain default
 hostname br7131-4AA708
 area RMZEcospace
 contact motorolasolutions
 country-code us
 channel-list 2.4GHz 1,2
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

Related Commands:

no	Removes the configured country code

floor

Device Config Commands

Sets the building floor where the device is deployed

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
floor <FLOOR-NAME>
```

Parameters

```
floor <FLOOR-NAME>
```

<FLOOR-NAME>	Sets the building floor where the device is deployed

Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#floor 5thfloor

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
br71xx 00-04-96-4A-A7-08
 use profile default-br71xx
 use rf-domain default
```

```
 hostname br7131-4AA708
 area RMZEcospace
 floor 5thfloor
 contact motorolasolutions
 country-code us
 channel-list 2.4GHz 1,2
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

Related Commands:

no	Removes device's location floor name

geo-coordinates

Device Config Commands

Configures the geographic coordinates for this device. Specifies the exact location of this device in terms of latitude and longitude coordinates.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
geographic coordinates <-90.0000-90.0000> <-180.0000-180.0000>
```

Parameters

```
geographic coordinates <-90.0000-90.0000> <-180.0000-180.0000>
```

geographic coordinates	Configures the geographic coordinates for this device • <-90.0000-90.0000> – Specify the device's latitude coordinate from -90.0000 to 90.0000. • <-180.0000-180.0000> – Specify the device's longitude coordinate from -180.0000 to 180.0000.

Example

```
rfs4000-229D58(config-device-00-23-68-22-9D-58)#geo-coordinates -90.0000 166
rfs4000-229D58(config-device-00-23-68-22-9D-58)#

rfs4000-229D58(config-device-00-23-68-22-9D-58)#show context
rfs4000 00-23-68-22-9D-58
 use profile default-rfs4000
 use rf-domain default
 hostname rfs4000-229D58
 geo-coordinates -90.0000 166.0000
 license AP DEFAULT-6AP-LICENSE
 license ADSEC DEFAULT-ADV-SEC-LICENSE
 ip default-gateway 192.168.13.2
 ip default-gateway priority static-route 20
 interface ge1
  switchport mode access
  switchport access vlan 1
```

```
 interface vlan1
  ip address 192.168.13.9/24
  ip address 192.168.0.1/24 secondary
  ip dhcp client request options all
 use client-identity-group ClientIdentityGroup
 logging on
 logging console warnings
 logging buffered warnings
rfs4000-229D58(config-device-00-23-68-22-9D-58)#
```

Related Commands:

no	Removes device's geographic coordinates

hostname

Device Config Commands

Sets the system's network name

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
hostname <WORD>
```

Parameters

```
hostname <WORD>
```

hostname <WORD>	Sets the name of the managing wireless controller, service platform, or access point. This name is displayed when accessed from any network.

Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#hostname TechPubAP7131

The hostname has changed from 'br7131-4AA708' to 'TechPubAP7131'

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
br71xx 00-04-96-4A-A7-08
 use profile default-br71xx
 use rf-domain default
 hostname TechPubAP7131
 area RMZEcospace
 floor 5thfloor
 contact motorolasolutions
 country-code us
 channel-list 2.4GHz 1,2
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

Related Commands:

no	Removes device's hostname

layout-coordinates

Device Config Commands

Configures X and Y layout coordinates for the device

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
layout-coordinates <-4096.0-4096.0> <-4096.0-4096.0>
```

Parameters

```
layout-coordinates <-4096.0-4096.0> <-4096.0-4096.0>
```

<-4096.0-4096.0>	Specify the X coordinate from -4096 - 4096.0
<-4096.0-4096.0>	Specify the Y coordinate from -4096 - 4096.0

Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#layout-coordinates 1 2

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
br71xx 00-04-96-4A-A7-08
 use profile default-br71xx
 use rf-domain default
 hostname TechPubAP7131
 area RMZEcospace
 floor 5thfloor
 layout-coordinates 1.0 2.0
 contact motorolasolutions
 country-code us
 channel-list 2.4GHz 1,2
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

Related Commands:

no	Removes device's layout co-ordinates

license

Device Config Commands

Adds a license pack on the device for the specified feature (AP/AAP/ADSEC/ADVANCED-WIPS/HTANLT/SMART-CACHE)

The Mobility HM network defines a three-tier structure, consisting of multiple wireless sites managed by a single *Network Operations Center* (NOC) controller, The NOC controller constitutes the first and the site controllers constitute the second tier of the hierarchy. The site controllers may or may not be grouped to form clusters. The site controllers in turn adopt and manage access points that form the third tier of the hierarchy.

The NOC controllers and/or site controllers can both have license packs installed. Adoption of APs by the NOC and site controllers depends on the number of licenses available on each of these controllers.

The NOC controllers and/or site controllers can both have license packs installed. When a AP is adopted by a site controller, the site controller pushes a license on to the AP. The various possible scenarios are:

- AP licenses installed only on NOC controller:

  The NOC controller provides the site controllers with AP licenses, ensuring that per platform limits are not exceeded.

- AP licenses installed on site controller:

  The site controller uses its installed licenses, and then asks the NOC controller for additional licenses in case of a shortage.

  In a hierarchical and centrally managed network, the NOC controller can pull unused AP licenses from site controllers and rellocate to other site controllers when required.

- AP licenses installed on any member of a site cluster:

  The site controller shares installed and borrowed (from the NOC) licenses with other controllers within a site cluster.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
license <WORD> <LICENSE-KEY>
```

Parameters

```
license <WORD> <LICENSE-KEY>
```

<WORD>	Specify the feature name (AP/AAP/ADSEC/ADVANCED-WIPS/HOTSPOT-ANALYTICS/SMART-CACHE) for which license is added
<LICENSE-KEY>	Specify the license key

Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#license br aplicensekey@1234
aplicensekey@123
```

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
br71xx 00-04-96-4A-A7-08
 use profile default-br71xx
 use rf-domain default
 hostname TechPubAP7131
 floor 5thfloor
 layout-coordinates 1.0 2.0
 license AP aplicensekey@1234 aplicensekey@123
 location Block3B
 no contact
 country-code us
 channel-list 2.4GHz 1,2
 mac-name 00-04-96-4A-A7-08 5.4TestAP
 neighbor-info-interval 50
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#

nx6524-858126(config-device-5C-0E-8B-85-81-26)#license ?
  WORD  Feature name (AP/AAP/ADSEC/ADVANCED-WIPS/HTANLT/SMART-CACHE) for which
        license is to be added
nx6524-858126(config-device-5C-0E-8B-85-81-26)#

nx6524-858126(config-device-5C-0E-8B-85-81-26)#license SMART-CACHE
29bedfa30cf4a5bcd20cd8815e00c948ddf26814e8346ef6f9e884832a7a49b349e6938f63ecf
653
nx6524-858126(config-device-5C-0E-8B-85-81-26)#commit

nx6524-858126(config-device-5C-0E-8B-85-81-26)#show licenses
Serial Number : 11185520500065

Device Licenses:
  AP-LICENSE
    String     :
29bedfa30cf4a5bce0c732a20e39f728ddf26814e8346ef6739f3ee2b1691d10246de8a11e439
131
...
  HOTSPOT-ANALYTICS
    String     :
29bedfa30cf4a5bcdf83ad26e814f39dddf26814e8346ef6f429383a6d51acd549e6938f63ecf
653
  SMART-CACHE
    String     :
29bedfa30cf4a5bcd20cd8815e00c948ddf26814e8346ef6f9e884832a7a49b349e6938f63ecf
653
--More--
nx6524-858126(config-device-5C-0E-8B-85-81-26)#
```

location

Device Config Commands

Sets the location where a managed device is deployed

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
location <WORD>
```

Parameters

```
location <WORD>
```

<WORD>	Specify the managed device's location of deployment

Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#location Block3B

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
br71xx 00-04-96-4A-A7-08
 use profile default-br71xx
 use rf-domain default
 hostname TechPubAP7131
 area RMZEcospace
 floor 5thfloor
 layout-coordinates 1.0 2.0
 location Block3B
 contact motorolasolutions
 country-code us
 channel-list 2.4GHz 1,2
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

Related Commands:

no	Removes a managed device's location

mac-name

Device Config Commands

Configures a MAC name for mappings

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
mac-name <MAC> <NAME>
```

Parameters

```
mac-name <MAC> <NAME>
```

<MAC> <NAME>	Configures a MAC address for the device • <NAME> – Set the 'friendly' name used for this MAC address

Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#mac-name 00-04-96-4A-A7-08
5.4TestAP

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
br71xx 00-04-96-4A-A7-08
 use profile default-br71xx
 use rf-domain default
 hostname TechPubAP7131
 area RMZEcospace
 floor 5thfloor
 layout-coordinates 1.0 2.0
 location Block3B
 contact motorolasolutions
 country-code us
 channel-list 2.4GHz 1,2
 mac-name 00-04-96-4A-A7-08 5.4TestAP
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

Related Commands:

no	Removes the device's friendly name to MAC address mapping

neighbor-info-interval

Device Config Commands

Configures neighbor information exchange interval

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
neighbor-info-interval <1-100>
```

Parameters

```
neighbor-info-interval <1-100>
```

neighbor-info-interval <1-100>	Sets neighbor information exchange interval • <1-100> – Specify a value from 1 - 100 seconds.

Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#neighbor-info-interval 50
```

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
br71xx 00-04-96-4A-A7-08
 use profile default-br71xx
 use rf-domain default
 hostname TechPubAP7131
 area RMZEcospace
 floor 5thfloor
 layout-coordinates 1.0 2.0
 location Block3B
 contact motorolasolutions
 country-code us
 channel-list 2.4GHz 1,2
 mac-name 00-04-96-4A-A7-08 5.4TestAP
 neighbor-info-interval 50
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

Related Commands:

no	Removes or reverts the device's settings

no

Device Config Commands

Negates a command or resets values to their default

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no [adopter-auto-provisioning-policy-lookup|adoption-site|area|arp|

auto-learn-staging-config|autoinstall|bridge|cdp|channel-list|cluster|

configuration-persistence|contact|controller|country-code|critical-resource|
          crypto|device-upgrade|dot1x|dscp-mapping|email-notification|

environmental-sensor|events|export|floor|geo-coordinates|gre|hostname|http-an
alyze|

interface|ip|l2tpv3|l3-lite-table|layout-coordinates|led|legacy-auto-downgrad
e|

legacy-auto-update|lldp|load-balancing|location|logging|mac-address-table|mac
-auth|

mac-name|memory-profile|meshpoint-device|meshpoint-monitor-interval|

min-misconfiguration-recovery-time|mint|mirror|misconfiguration-recovery-time
|
```

```
network-alias|noc|ntp|override-wlan|power-config|preferred-controller-group|

preferred-tunnel-controller|radius|rf-domain-manager|router|rsa-key|sensor-se
rver|
          slot|spanning-tree|timezone|trustpoint|tunnel-controller|use|vrrp|
          wep-shared-key-auth|service]
```

Parameters

None

Usage Guidelines:

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated

Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#no area

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#no contact
```

Related Commands:

adopter-auto-provisioning-policy-lookup	Enables the use of a centralized auto provisioning policy on this profile or device
adoption-site	Sets the device's adoption site name
alias	Creates a network, VLAN, and service alias and enters its configuration mode
area	Sets the name of area where the system is deployed
arp	Configures ARP parameters
auto-learn-staging-config	Enables the automatic recognition of devices pending adoption
autoinstall	Autoinstalls firmware image and configuration setup parameters
bridge	Configures Ethernet Bridging parameters
cdp	Operates CDP on the device
channel-list	Configures channel list advertised to wireless clients
cluster	Sets cluster configuration
configuration-persistence	Enables configuration persistence across reloads
contact	Sets contact information
controller	Configures controller WLAN settings
country-code	Configures the two digit country code for legal operation
crypto	Configures crypto settings
device-upgrade	Configures device firmware upgrade settings on this device
dot1x	Configures 802.1x standard authentication controls
dscp-mapping	Configures IP *Differentiated Services Code Point* (DSCP) to 802.1p priority mapping for untagged frames
email-notification	Configures e-mail notification

enforce-version	Checks the device firmware version before attempting connection
environmental-sensor	Configures the environmental sensor device settings. If the device is an environmental sensor, use this command to configures its settings,
events	Displays system event messages
export	Enables export of startup.log file after every boot
floor	Sets the building floor where the system is deployed
geo-coordinates	Configures the geographic coordinates for this device
gre	Enables GRE tunneling on this profile
hostname	Sets a system's network name
http-analyze	Enables HTTP analysis on this device
interface	Selects an interface to configure
ip	Configures IP components
l2tpv3	Defines the L2TP protocol for tunneling layer 2 payloads using VPNs
l3e-lite-table	Configures L3e lite table aging time
layout-coordinates	Configures layout coordinates
led	Turns LEDs on or off
legacy-auto-downgrade	Enables legacy device firmware to auto downgrade
legacy-auto-update	Auto updates Brocade Mobility 650 Access Point and Brocade Mobility 71XX Access Point legacy device firmware
lldp	Configures LLDP settings for this profile
load-balancing	Configures load balancing parameters
location	Configures the location the system is deployed
logging	Enables message logging
mac-address-table	Configures the MAC address table
mac-auth	Enables 802.1x authentication of hosts on this device
mac-name	Configures MAC name to name mappings
memory-profile	Configures device's memory profile
meshpoint-device	Configures device's meshpoint parameters
meshpoint-monitor-interval	Configures meshpoint monitoring interval on the device
min-misconfiguration-recovery-time	Configures the minimum connectivity verification time
mint	Configures MiNT protocol commands
misconfiguration-recovery-time	Verifies connectivity after a device configuration is received
neighbor-inactivity-timeout	Configures a neighbor inactivity timeout
neighbor-info-interval	Configures the neighbor information exchange interval
noc	Configures NOC settings
ntp	Configure the NTP server settings

override-wlan	Configures WLAN RF Domain level overrides
power-config	Configures power mode features
preferred-controller-group	Specifies the group the system prefers for adoption
preferred-tunnel-controller	Configures the tunnel preferred by the system for tunneling extended VLAN traffic
radius	Configures device-level RADIUS authentication parameters
remove-override	Removes device overrides
rf-domain-manager	Enables the RF Domain manager
router	Configures dynamic router protocol settings
rsa-key	Assigns a RSA key to SSH
sensor-server	Configures an AirDefense sensor server
spanning-tree	Enables spanning tree commands
timezone	Configures time zone settings
trustpoint	Assigns a trustpoint to a service
tunnel-controller	Configures the tunneled WLAN (extended VLAN) wireless controller or service platform's name
use	Defines the settings used by this feature
vrrp	Configures VRRP group settings
wep-shared-key-auth	Enables support for 802.11 WEP shared key authentication
clrscr	Clears the display screen
commit	Commits (saves) changes made in the current session
end	Ends and exits the current mode and moves to the PRIV EXEC mode
exit	Ends the current mode and moves to the previous mode
help	Displays the interactive help system
revert	Reverts changes to their last saved configuration
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations
show	Displays running system information
write	Writes information to memory or terminal

override-wlan

Device Config Commands

Configures WLAN RF Domain level overrides

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
override-wlan <WLAN> [ssid|vlan-pool|wpa-wpa2-psk]
override-wlan <WLAN> [ssid <SSID>|vlan-pool <1-4094> {limit <0-8192>}|
          wpa-wpa2-psk <WORD>]
```

Parameters

```
override-wlan WLAN [ssid <SSID>|vlan-pool <1-4094> {limit <0-8192>}|
wpa-wpa2-psk <WORD>]
```

<WLAN>	Specify the WLAN name. Configure the following WLAN parameters: SSID, VLAN pool, and WPA-WPA2 key.
SSID <SSID>	Configures the WLAN *Service Set Identifier* (SSID) • <SSID> – Specify an SSID ID.
vlan-pool <1-4094> {limit <0-8192>}	Configures a pool of VLANs for the selected WLAN • <1-4094> – Specifies a VLAN pool ID from 1 - 4094. • limit – Optional. Limits the number of users on this VLAN pool • <0-8192> – Specify the user limit from 0 - 8192. **NOTE:** The VLAN pool configuration overrides the VLAN configuration.
wpa-wpa2-psk <WORD>	Configures the WLAN WPA-WPA2 key or passphrase for the selected WLAN • <WORD> – Specify a WPA-WPA2 key or passphrase.

Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#override-wlan test vlan-pool
8

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
br71xx 00-04-96-4A-A7-08
 use profile default-br71xx
 use rf-domain default
 hostname TechPubAP7131
 floor 5thfloor
 layout-coordinates 1.0 2.0
 license AP aplicenseley@1234 aplicensekey@123
 location Block3B
 no contact
 country-code us
 channel-list 2.4GHz 1,2
 override-wlan test vlan-pool 8
 mac-name 00-04-96-4A-A7-08 5.4TestAP
 neighbor-info-interval 50
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

Related Commands:

no	Removes RF Domain level WLAN overrides

remove-override

Device Config Commands

Removes device overrides

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
remove-override <PARAMETERS>
```

Parameters

None

Example

```
rfs4000-229D58(config-device-00-23-68-22-9D-58)#remove-override ?
  adopter-auto-provisioning-policy-lookup  Use centralized auto-provisioning
                                           policy when adopted by another
                                           controller
  alias                                    Alias
  all                                     Remove all overrides for the device
  area                                   Reset name of area where the system is
                                           located
  arp                                      Address Resolution Protocol (ARP)
  auto-learn-staging-config                Enable learning network
configuration
                                          of the devices that come for adoption
  autoinstall                              Autoinstall settings
  bridge                                   Bridge group commands
  captive-portal                           Captive portal
  cdp                                      Cisco Discovery Protocol
  channel-list                             Configure a channel list to be
                                           advertised to wireless clients
  cluster                                  Cluster configuration
  configuration-persistence                Automatic write of startup
                                           configuration file
  contact                                  The contact
  controller                               WLAN controller configuration
  country-code                             The country of operation
  critical-resource                        Critical Resource
  crypto                                   Encryption related commands
  device-upgrade                           Device firmware upgrade
  dot1x                                    802.1X
  dscp-mapping                           IP DSCP to 802.1p priority mapping for
                                           untagged frames
  email-notification                       Email notification configuration
  enforce-version                          Check the firmware versions of
devices
                                           before interoperating
  environmental-sensor                    Environmental Sensors Configuration
  events                                   System event messages
  export                                   Export a file
  firewall                                 Enable/Disable firewall
  floor                                   Reset name of floor where the system
                                           is located
  global                                 Remove global overrides for the device
                                           but keeps per-interface overrides
```

```
  gre                                    GRE protocol
  interface                              Select an interface to configure
  ip                                     Internet Protocol (IP)
  l2tpv3                                 L2tpv3 protocol
  l3e-lite-table                         L3e lite Table
  led                                    LED on the device
  lldp                                   Link Layer Discovery Protocol
  location                               The location
  logging                                Modify message logging facilities
  mac-address-table                      MAC Address Table
  mac-auth                               802.1X
  memory-profile                         Memory-profile
  mint                                   MiNT protocol
  noc                                    Noc related configuration
  ntp                                    Configure NTP
  override-wlan                          Overrides for wlans
  power-config                           Configure power mode
  preferred-controller-group             Controller group this system will
                                         prefer for adoption
  preferred-tunnel-controller            Tunnel Controller Name this system
                                         will prefer for tunneling extended
                                         vlan traffic
  rf-domain-manager                      RF Domain Manager
  router                                 Dynamic routing
  routing-policy                         Policy Based Routing Configuration
  sensor-server                        Motorola AirDefense WIPS sensor server
                                         configuration
  spanning-tree                          Spanning tree
  timezone                               The timezone
  tunnel-controller                      Tunnel Controller group this
                                         controller belongs to
  use                                    Set setting to use
  vrrp                                   VRRP configuration

  service                                Service Commands

rfs4000-229D58(config-device-00-23-68-22-9D-58)#
```

rsa-key

Device Config Commands

Assigns a RSA key to a device

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
rsa-key ssh <RSA-KEY-NAME>
```

Parameters

```
rsa-key ssh <RSA-KEY-NAME>
```

ssh <RSA-KEY-NAME>	Assigns RSA key to SSH • <RSA-KEY-NAME> – Specifies the RSA key name. The key should be installed using PKI commands in the enable mode.

Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#rsa-key ssh rsa-key1

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
br71xx 00-04-96-4A-A7-08
 use profile default-br71xx
 use rf-domain default
 hostname TechPubAP7131
 floor 5thfloor
 layout-coordinates 1.0 2.0
 license AP aplicenseley@1234 aplicensekey@123
 rsa-key ssh rsa-key1
 location Block3B
 no contact
 country-code us
 channel-list 2.4GHz 1,2
 override-wlan test vlan-pool 8
 mac-name 00-04-96-4A-A7-08 5.4TestAP
 neighbor-info-interval 50
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

Related Commands:

no	Removes RSA key from service

sensor-server

Device Config Commands

Configures an AirDefense sensor server

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
sensor-server <1-3> ip <IP> {port [443|8443|<1-65535>]}
```

Parameters

```
sensor-server <1-3> ip <IP> {port [443|8443|<1-65535>]}
```

sensor-server <1-3>	Selects a sensor server to configure

ip <IP>	Configures sensor server's IP address • <IP> – Specify the IP address.
port [443|8443|<1-65535>]	Optional. Configures the port. The options are: • 443 – The default port used by the AirDefense server • 8443 – The default port used by advanced WIPS • <1-65535> – Manually sets the port number of the advanced WIPS/AirDefense server

Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#sensor-server 1 ip
172.16.10.7

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
br71xx 00-04-96-4A-A7-08
 use profile default-br71xx
 use rf-domain default
 hostname TechPubAP7131
 floor 5thfloor
 layout-coordinates 1.0 2.0
 license AP aplicenseley@1234 aplicensekey@123
 rsa-key ssh rsa-key1
 location Block3B
 no contact
 country-code us
 sensor-server 1 ip 172.16.10.7
 channel-list 2.4GHz 1,2
 override-wlan test vlan-pool 8
 mac-name 00-04-96-4A-A7-08 5.4TestAP
 neighbor-info-interval 50
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

Related Commands:

no	Removes configured sensor server

timezone

Device Config Commands

Configures device's timezone

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
timezone <TIMEZONE>
```

Parameters

```
timezone <TIMEZONE>
```

timezone <TIMEZONE>	Configures the device's timezone

Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#timezone Etc/UTC

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
br71xx 00-04-96-4A-A7-08
 use profile default-br71xx
 use rf-domain default
 hostname TechPubAP7131
 floor 5thfloor
 layout-coordinates 1.0 2.0
 license AP aplicenseley@1234 aplicensekey@123
 rsa-key ssh rsa-key1
 location Block3B
 no contact
 timezone Etc/UTC
 stats open-window 2 sample-interval 77 size 10
 country-code us
 sensor-server 1 ip 172.16.10.7
 channel-list 2.4GHz 1,2
 override-wlan test vlan-pool 8
 mac-name 00-04-96-4A-A7-08 5.4TestAP
 neighbor-info-interval 50
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

Related Commands:

no	Removes device's configured timezone

trustpoint

Device Config Commands

Assigns a trustpoint

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
trustpoint [https|radius-ca|radius-server] <TRUSTPOINT>
```

Parameters

```
trustpoint [https|radius-ca|radius-server] <TRUSTPOINT>
```

https <TRUSTPOINT>	Assigns a specified trustpoint to HTTPS • <TRUSTPOINT> – Specify the trustpoint name.
radius-ca <TRUSTPOINT>	Assigns a trustpoint as a certificate authority for validating client certificates in EAP • <TRUSTPOINT> – Specify the trustpoint name.
radius-server <TRUSTPOINT>	Specifies the name of the trustpoint. Install the trustpoint using PKI commands in the enable mode. • <TRUSTPOINT> – Specify the trustpoint name.

Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#trustpoint radius-ca trust2

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
br71xx 00-04-96-4A-A7-08
 use profile default-br71xx
 use rf-domain default
 hostname TechPubAP7131
 floor 5thfloor
 layout-coordinates 1.0 2.0
 license AP aplicenseley@1234 aplicensekey@123
 trustpoint radius-ca trust2
 rsa-key ssh rsa-key1
 location Block3B
 no contact
 timezone Etc/UTC
 stats open-window 2 sample-interval 77 size 10
 country-code us
 sensor-server 1 ip 172.16.10.7
 channel-list 2.4GHz 1,2
 override-wlan test vlan-pool 8
 mac-name 00-04-96-4A-A7-08 5.4TestAP
 neighbor-info-interval 50
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

Related Commands:

no	Removes configured trustpoint from service

Chapter

AAA-POLICY

8

This chapter summarizes the *Authentication, Authorization, and Accounting (*AAA) policy commands in the CLI command structure.

A AAA policy enables administrators to define access control settings governing network permissions. External RADIUS and LDAP servers (AAA servers) also provide user database information and user authentication data. Each WLAN maintains its own unique AAA configuration.

AAA provides a modular way of performing the following services:

Authentication — Provides a means for identifying users, including login and password dialog, challenge and response, messaging support and (depending on the security protocol), encryption. Authentication is the technique by which a user is identified before allowed access to the network. Configure AAA authentication by defining a list of authentication methods, and then applying the list to various interfaces. The list defines the authentication schemes performed and their sequence. The list must be applied to an interface before the defined authentication technique is conducted.

Authorization — Authorization occurs immediately after authentication. Authorization is a method for remote access control, including authorization for services and individual user accounts and profiles. Authorization functions through the assembly of attribute sets describing what the user is authorized to perform. These attributes are compared to information contained in a database for a given user and the result is returned to AAA to determine the user's actual capabilities and restrictions. The database could be located locally or be hosted remotely on a RADIUS server. Remote RADIUS servers authorize users by associating *attribute-value* (AV) pairs with the appropriate user. Each authorization method must be defined through AAA. When AAA authorization is enabled it's applied equally to all interfaces.

Accounting — Collects and sends security server information for billing, auditing, and reporting user data; such as start and stop times, executed commands (such as PPP), number of packets, and number of bytes. Accounting enables wireless network administrators to track the services users are accessing and the network resources they are consuming. When accounting is enabled, the network access server reports user activity to a RADIUS security server in the form of accounting records. Each accounting record is comprised of AV pairs and is stored locally on the access control server. The data can be analyzed for network management, client billing, and/or auditing. Accounting methods must be defined through AAA. When AAA accounting is activated, it is applied equally to all interfaces on the access servers.

Use the (config) instance to configure AAA policy commands. To navigate to the config-aaa-policy instance, use the following commands:

```
<DEVICE>(config)#aaa-policy <POLICY-NAME>

rfs7000-37FABE(config)#aaa-policy test

rfs7000-37FABE(config-aaa-policy-test)#?
AAA Policy Mode commands:
  accounting           Configure accounting parameters
  attribute            Configure RADIUS attributes in access and accounting
                       requests
```

```
  authentication       Configure authentication parameters
  health-check         Configure server health-check parameters
  mac-address-format   Configure the format in which the MAC address must be
                       filled in the Radius-Request frames
  no                   Negate a command or set its defaults
  proxy-attribute      Configure radius attribute behavior when proxying
                       through controller or rf-domain-manager
  server-pooling-mode  Configure the method of selecting a server from the
                       pool of configured AAA servers
  use                  Set setting to use

  clrscr               Clears the display screen
  commit               Commit all changes made in this session
  do                   Run commands from Exec mode
  end                  End current mode and change to EXEC mode
  exit                 End current mode and down to previous mode
  help                 Description of the interactive help system
  revert               Revert changes
  service              Service Commands
  show                 Show running system information
  write                Write running configuration to memory or terminal

rfs7000-37FABE(config-aaa-policy-test)#
```

aaa-policy

Table 6 summarizes AAA policy configuration commands.

TABLE 6 AAA-Policy-Config Commands

Command	Description	Reference
accounting	Configures accounting parameters	*page 8-833*
attribute	Configure RADIUS attributes in access and accounting requests	page 836
authentication	Configures authentication parameters	page 838
health-check	Configures health check parameters	page 842
mac-address-format	Configures the MAC address format	page 843
no	Negates a command or sets its default	page 844
proxy-attribute	Configures the RADIUS server's attribute behavior when proxying through the wireless controller or the RF Domain manager	page 848
server-pooling-mode	Defines the method for selecting a server from the pool of configured AAA servers	page 849
use	Defines the AAA command settings	page 850
clrscr	Clears the display screen	*page 5-385*
commit	Commits (saves) changes made in the current session	*page 5-386*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-234*
exit	Ends the current mode and moves to the previous mode	*page 5-387*
help	Displays the interactive help system	*page 5-387*
revert	Reverts changes to their last saved configuration	*page 5-394*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 5-394*

TABLE 6 AAA-Policy-Config Commands

Command	Description	Reference
show	Displays running system information	*page 6-429*
write	Writes information to memory or terminal	*page 5-425*

accounting

aaa-policy

Configures the server type and interval at which interim accounting updates are sent to the server. A maximum of 6 accounting servers can be configured.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
accounting [interim|server|type]

accounting interim interval <60-3600>

accounting server [<1-6>|preference]

accounting server preference [auth-server-host|auth-server-number|none]

accounting server <1-6> [dscp|host|nai-routing|onboard|proxy-mode|
          retry-timeout-factor|timeout]
accounting server <1-6> [dscp <0-63>|retry-timeout-factor <50-200>]
accounting server <1-6> host <IP/HOSTNAME> secret [0 <SECRET>|2
<SECRET>|<SECRET>]
  {port <1-65535>}
accounting server <1-6> nai-routing realm-type [prefix|suffix] realm
<REALM-TEXT>
  {strip}
accounting server <1-6> onboard [self|controller]
accounting server <1-6> proxy-mode [none|through-controller|through-mint-host
          <HOSTNAME/MINT-ID>|through-rf-domain-manager]
accounting server <1-6> timeout <1-60> {attempts <1-10>}

accounting type [start-interim-stop|start-stop|stop-only]
```

Parameters

```
accounting interim interval <60-3600>
```

interim	Configures the interim accounting interval
interval <60-3000>	Specify the interim interval from 60 - 3600 seconds. The default is 1800 seconds.

	`accounting server preference [auth-server-host|auth-server-number|none]`
server	Configures a RADIUS accounting server's settings
preference	Configures the accounting server's preference mode. Authentication requests are forwarded to a accounting server, from the pool, based on the preference mode selected.
auth-server-host	Sets the authentication server as the accounting server This parameter indicates the same server is used for authentication and accounting. The server is identified by its hostname.
auth-server-number	Sets the authentication server as the accounting server This parameter indicates the same server is used for authentication and accounting. The server is identified by its index or number.
none	Indicates the accounting server is independent of the authentication server
	`accounting server <1-6> [dscp <0-63>|retry-timeout-factor <50-200>]`
server <1-6>	Configures an accounting server. Up to 6 accounting servers can be configured.
dscp <0-63>	Sets the *Differentiated Services Code Point* (DSCP) value for *Quality of Service* (QOS) monitoring. This value is used in generated RADIUS packets. • <0-63> – Sets the DSCP value from 0 - 63
retry-timeout-factor <50-200>	Sets the scaling factor for retransmission timeouts. The timeout at each attempt is a function of this retry-timeout factor and the attempt number. • <50-200> – Specify a value from 50 - 200. The default is 100. If the scaling factor is 100, the interval between two consecutive retries remains the same, irrespective of the number of retries. If the scaling factor is less than 100, the interval between two consecutive retires reduces with subsequent retries. If this scaling factor is greater than 100, the interval between two consecutive retries increases with subsequent retries.
	`accounting server <1-6> host <IP/HOSTNAME> secret [0 <SECRET>|2 <SECRET>|<SECRET>]` *`{port <1-65535>}`*
server <1-6>	Configures an accounting server. Up to 6 accounting servers can be configured.
host <IP/HOSTNAME>	Configures the accounting server's hostname or IP address
secret [0 <SECRET>| 2 <SECRET>| <SECRET>]	Configures a common secret key used to authenticate with the accounting server • 0 <SECRET> – Configures a clear text secret key • 2 <SECRET> – Configures an encrypted secret key • <SECRET> – Specify the secret key. This shared secret should not exceed 127 characters.
port <1-65535>	Optional. Configures the accounting server's UDP port (the port used to connect to the accounting server) • <1-65535> – Sets the port number from 1 - 65535 (default port is 1813)
	`accounting server <1-6> nai-routing realm-type [prefix|suffix] realm <REALM-TEXT>` *`{strip}`*
server <1-6>	Configures an accounting server. Up to 6 accounting servers can be configured.
nai-routing	Enables *Network Access Identifier* (NAI) routing The NAI is a character string in the format of an e-mail address as either user or user@ (it need not be a valid e-mail address or a *fully qualified domain name* (FQDN). The NAI can be used either in a specific or generic form. The specific form, which must contain the user portion and may contain the @ portion, identifies a single user. The generic form allows to be configured on a single command line. Each user still needs a unique security association, but these associations can be stored on a AAA server. The original purpose of NAI was to support roaming between dial up ISPs. Using NAI, each ISP need not have all the accounts for all of its roaming partners in a single RADIUS database. RADIUS servers can proxy requests to remote servers.

realm-type	Selects the match type used on the username
[prefix|suffix]	Select one of the following options: • prefix – Matches the prefix of the username (For example, username is of type DOMAIN/user1, DOMAIN/user2). This is the default setting. • suffix – Matches the suffix of the username (For example, user1@DOMAIN, user2)@DOMAIN)
realm <REALM-TEXT>	Configures the text matched against the username. Enter the realm name (should not exceed 50 characters). When the RADIUS accounting server receives a request for a user name, the server references a table of user names. If the user name is known, the server proxies the request to the RADIUS server. • <REALM-TEXT> – Specifies the matching text including the delimiter (a delimiter is typically " or '@')
strip	Optional. Strips the realm from the username before forwarding the request to the RADIUS server

```
accounting server <1-6> onboard [self|controller]
```

server <1-6>	Configures an accounting server. Up to 6 accounting servers can be configured.
onboard	Selects an onboard server instead of an external host
self	Configures the onboard server on a AP, wireless controller, or service platform (where the client is associated)
controller	Configures local RADIUS server settings

```
accounting server <1-6> proxy-mode [none|through-controller|through-mint-host
<HOSTNAME/MINT-ID>|through-rf-domain-manager]
```

server <1-6>	Configures an accounting server. Up to 6 accounting servers can be configured.
proxy-mode	Select the mode used to proxy requests. The options are: none, through-controller, and through-rf-domain-manager.
none	No proxy required. Sends the request directly using the IP address of the device
through-controller	Proxies requests through the controller (access point, wireless controller, or service platform) configuring the device
through-mint-host <HOSTNAME/MINT-ID>	Proxies requests through a neighboring MiNT device. Provide the device's MiNT ID or hostname.
through-rf-domain-manager	Proxies requests through the local RF Domain Manager

```
accounting server <1-6> timeout <1-60> {attempts <1-10>}
```

server <1-6>	Configures an accounting server. Up to 6 accounting servers can be configured.
timeout <1-60>	Configures the timeout for each request sent to the RADIUS server • <1-60> – Specify a value from 1 - 60 seconds.
attempts <1-10>	Optional. Specifies the number of times a transmission request is attempted • <1-10> – Specify a value from 1 - 10.

```
accounting type [start-interim-stop|start-stop|stop-only]
```

type	Configures the type of RADIUS accounting packets sent. The options are: start-interim-stop, start-stop, and stop-only.
start-interim-stop	Sends accounting-start and accounting-stop messages when the session starts and stops. This parameter also sends interim accounting updates.
start-stop	Sends accounting-start and accounting-stop messages when the session starts and stops. This is the default setting.
stop-only	Sends an accounting-stop message when the session ends

Example

```
rfs7000-37FABE(config-aaa-policy-test)#accounting interim interval 65

rfs7000-37FABE(config-aaa-policy-test)#accounting server 2 host 172.16.10.10
secret example port 1
rfs7000-37FABE(config-aaa-policy-test)#accounting server 2 timeout 2 attempts
2
rfs7000-37FABE(config-aaa-policy-test)#accounting type start-stop
rfs7000-37FABE(config-aaa-policy-test)#accounting server preference
auth-server-number

rfs7000-37FABE(config-aaa-policy-test)#show context
aaa-policy test
 accounting server 2 host 172.16.10.10 secret 0 example port 1
 accounting server 2 timeout 2 attempts 2
 accounting interim interval 65
 accounting server preference auth-server-number
rfs7000-37FABE(config-aaa-policy-test)#
```

Related Commands:

no	Removes or resets accounting server parameters

attribute

aaa-policy

Configures RADIUS Framed-MTU attribute used in access and accounting requests. The Framed-MTU attribute reduces the *Extensible Authentication Protocol* (EAP) packet size of the RADIUS server. This command is useful in networks where routers and firewalls do not perform fragmentation.

To ensure network security, some firewall software drop UDP fragments from RADIUS server EAP packets. Consequently, the packets are large. Using Framed MTU reduces the packet size. EAP authentication uses Framed MTU to notify the RADIUS server about the *Maximum Transmission Unit* (MTU) negotiation with the client. The RADIUS server communications with the client do not include EAP messages that cannot be delivered over the network.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
attribute
[acct-delay-time|acct-multi-session-id|chargeable-user-identity|cisco-vsa|

framed-mtu|location-information|nas-ipv6-address|operator-name|service-type]

attribute acct-delay-time
attribute acct-multi-session-id
```

```
attribute chargeable-user-identity
attribute cisco-vsa audit-session-id
attribute framed-mtu <100-1500>
attribute location-information [include-always|none|server-requested]
attribute nas-ipv6-address
attribute operator-name <OPERATOR-NAME>
attribute service-type [framed|login]
```

Parameters

`attribute acct-delay-time`

acct-delay-time	Enables support for *accounting-delay-time* attribute in accounting requests. When enabled, this attribute indicates the number of seconds the client has been trying to send a request to the accounting server. By subtracting this value from the time the packet is received by the server, the system is able to calculate the time of a request-generating event. Note, the network transit time is ignored. Including the *acct-delay-time* attribute in accounting requests updates the acct-delay-time value whenever the packet is retransmitted, This changes the content of the attributes field, requiring a new identifier and request authenticator.

`attribute acct-multi-session-id`

acct-multi-session-id	Enables support for *accounting-multi-session-id* attribute. When enabled, it allows linking of multiple related sessions of a roaming client. This option is useful in scenarios where a client roaming between access points sends multiple RADIUS accounting requests to different access points.

`attribute chargeable-user-identity`

chargeable-user-identity	Enables support for chargeable-user-identity attribute

`attribute cisco-vsa audit-session-id`

cisco-vsa audit-session-id	Configures the CISCO *Vendor Specific Attribute* (VSA) attribute included in access requests. This feature s disabled by default. This VSA allows CISCO's *Identity Services Engine* (ISE) to validate a requesting client's network compliance, such as the validity of virus definition files (antivirus software or definition files for an anti-spyware software application). • audit-session-id – Includes the audit session ID attribute in access requests The audit session ID is included in access requests when Cisco ISE is configured as an authentication server. **NOTE:** If the Cisco VSA attribute is enabled, configure an additional UDP port to listen for dynamic authorization messages from the Cisco ISE server. For more information, see *service*.

`attribute framed-mtu <100-1500>`

framed-mtu <100-1500>	Configures Framed-MTU attribute used in access requests • <100-1500> – Specify the Framed-MTU attribute from 100 - 1500.

`attribute location-information [include-always|none|server-requested]`

location-information [include-always| none|server-requested]	Enables/disables support for RFC5580 location information attribute, based on the option selected. The various options are: • include-always – Always includes location information in RADIUS authentication and accounting messages • none – Disables sending of location information in RADIUS authentication and accounting messages • server-requested – Includes location information in RADIUS authentication and accounting messages only when requested by the server When enabled, location information is exchanged in authentication and accounting messages.

	`attribute nas-ipv6-address`
nas-ipv6-address	Enables support for NAS IPv6 address When enabled, IPv6 addresses are assigned to hosts. The length of IPv4 and IPv6 addresses is 32-bit and 128-bit respectively. Consequently, an IPv6 address requires a larger address space.

	`attribute operator-name <OPERATOR-NAME>`
operator-name <OPERATOR-NAME>	Enables support for RFC5580 operator name attribute. When enabled, the network operator's name is included in all RADIUS authentication and accounting messages and uniquely identifies the access network owner. • <OPERATOR-NAME> – Specify the network operator's name.

	`attribute service-type [framed|login]`
service-type [framed|login]	Configures the service-type (6) attribute value. This attribute identifies the following: the type of service requested and the type of service to be provided. • framed – Sets service-type to *framed (2)* in the authentication packets. When enabled, a framed protocol, *Point-to-Point Protocol* (PPP) or *Serial Line Internet Protocol* (SLIP), is started for the client. • login – Sets service-type to *login (1)* in the authentication packets. When enabled, the client is connected to the host.

Example

```
rfs7000-37FABE(config-aaa-policy-test)#attribute framed-mtu 110
rfs7000-37FABE(config-aaa-policy-test)#show context
aaa-policy test
 accounting server 2 host 172.16.10.10 secret 0 example port 1
 accounting server 2 timeout 2 attempts 2
 accounting interim interval 65
 accounting server preference auth-server-number
 attribute framed-mtu 110
rfs7000-37FABE(config-aaa-policy-test)#

rfs7000-37FABE(config-aaa-policy-test1)#attribute cisco-vsa audit-session-id

rfs7000-37FABE(config-aaa-policy-test1)#show context
aaa-policy test
 attribute cisco-vsa audit-session-id
rfs7000-37FABE(config-aaa-policy-test)#
```

Related Commands:

no	Resets values or disables commands

authentication

aaa-policy

Configures user authentication parameters

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
authentication [eap|protocol|server]

authentication eap wireless-client [attempts
<1-10>|identity-request-retry-timeout
          <10-5000>|identity-request-timeout <1-60>|retry-timeout-factor
<50-200>|
          timeout <1-60>]

authentication protocol [chap|mschap|mschapv2|pap]

authentication server <1-6> [dscp|host|nac|nai-routing|onboard|proxy-mode|
          retry-timeout-factor|timeout]

authentication server <1-6> dscp <0-63>
authentication server <1-6> host <IP/HOSTNAME> secret [0 <SECRET>|2
<SECRET>|<SECRET>]
          {port <1-65535>}
authentication server <1-6> nac
authentication server <1-6> nai-routing realm-type [prefix|suffix] realm
<REALM-NAME>
          {strip}
authentication server <1-6> onboard [controller|self]
authentication server <1-6> proxy-mode
[none|through-controller|through-mint-host
          <HOSTNAME/MINT-ID>|through-rf-domain-manager]
authentication server <1-6> retry-timeout-factor <50-200>
authentication server <1-6> timeout <1-60> {attempts <1-10>}
```

Parameters

```
authentication eap wireless-client [attempts
<1-10>|identity-request-retry-timeout
<10-5000>|identity-request-timeout <1-60>|retry-timeout-factor <50-200>|
timeout <1-60>]
```

eap	Configures EAP authentication parameters
wireless-client	Configures wireless client's EAP parameters
attempts <1-10>	Configures the maximum number of attempts allowed to authenticate a wireless client • <1-10> – Specify a value from 1 - 10. The default is 3.
identity-request-retry-timeout <10-5000>	Configures the interval, in milliseconds, after which an EAP-identity request to the wireless client is retried • <10-5000> – Specify a value from 10 - 5000 milliseconds.
identity-request-timeout <1-60>	Configures the timeout, in seconds, after the last EAP-identity request message retry attempt (to allow time to manually enter user credentials) • <1-60> – Specify a value from 1 - 60 seconds. The default is 3 seconds.

retry-timeout-factor <50-200>	Configures the spacing between successive EAP retries • <50-200> – Specify a value from 50 - 200. The default is 100. A value of 100 indicates the interval between two consecutive retires remains the same irrespective of the number of retries. A value lesser than 100 indicates the interval between two consecutive retries reduces with each successive retry. A value greater than 100 indicates the interval between two consecutive retries increases with each successive retry.
timeout <1-60>	Configures the interval, in seconds, between successive EAP-identity request sent to a wireless client • <1-60> – Specify a value from 1 - 60 seconds.

`authentication protocol [chap|mschap|mschapv2|pap]`

protocol [chap|mschap|mschapv2|pap]	Configures one of the following protocols for non-EAP authentication: • chap – Uses *Challenge Handshake Authentication Protocol* (CHAP) • mschap – Uses *Microsoft Challenge Handshake Authentication Protocol* (MS-CHAP) • mschapv2 – Uses MS-CHAP version 2 • pap – Uses *Password Authentication Protocol* (PAP) (default authentication protocol used)

`authentication server <1-6> dscp <0-63>`

server <1-6>	Configures a RADIUS authentication server. Up to 6 RADIUS servers can be configured. • <1-6> – Specify the RADIUS server index from 1 - 6.
dscp <0-63>	Configures the *Differentiated Service Code Point* (DSCP) quality of service parameter generated in RADIUS packets. The DSCP value specifies the class of service provided to a packet, and is represented by a 6-bit parameter in the header of every IP packet. The default is 46.

`authentication server <1-6> host <IP/HOSTNAME> secret [0 <SECRET>|2 <SECRET>|<SECRET>] {port <1-65535>}`

server <1-6>	Configures a RADIUS authentication server. Up to 6 RADIUS servers can be configured. • <1-6> – Specify the RADIUS server index from 1 - 6.
host <IP/HOSTNAME>	Sets the RADIUS authentication server's IP address or hostname
secret [0 <SECRET>|2 <SECRET>|<SECRET>]	Configures the RADIUS authentication server's secret. This key is used to authenticate with the RADIUS server. • 0 <SECRET> – Configures a clear text secret • 2 <SECRET> – Configures an encrypted secret • <SECRET> – Specify the secret key. The shared key should not exceed 127 characters.
port <1-65535>	Optional. Specifies the RADIUS authentication server's UDP port (this port is used to connect to the RADIUS server) • <1-65535> – Specify a value from 1 - 65535. The default port is 1812.

`authentication server <1-6> nac`

server <1-6>	Configures a RADIUS authentication server. Up to 6 RADIUS servers can be configured. • <1-6> – Specify the RADIUS server index from 1 - 6.
nac	Enables *Network Access Control* (NAC) on the RADIUS authentication server identified by the <1-6> parameter. Using NAC, the controller hardware and software grant access to specific network resources. NAC performs a user and client authorization check for resources that do not have a NAC agent. NAC verifies the client's compliance with the controller's security policy. The controller supports only the EAP/802.1x type of NAC. However, the controller also provides a means to bypass NAC authentication for client's that do not have NAC 802.1x support (printers, phones, PDAs etc.).

	`accounting server <1-6> nai-routing realm-type [prefix|suffix] realm <REALM-NAME> {strip}`
server <1-6>	Configures a RADIUS authentication server. Up to 6 RADIUS servers can be configured. • <1-6> – Specifies the RADIUS server index from 1 - 6.
nai-routing	Enables NAI routing. When enabled, AAA servers identify clients using NAI. The NAI is a character string in the format of an e-mail address as either user or user@ but it need not be a valid e-mail address or a fully qualified domain name. The NAI can be used either in a specific or generic form. The specific form, which must contain the user portion and may contain the @ portion, identifies a single user. The generic form allows all users in a given or without a to be configured on a single command line. Each user still needs a unique security association, but these associations can be stored on a AAA server. The original purpose of the NAI was to support roaming between dial up ISPs. Using NAI, each ISP need not have all the accounts for all of its roaming partners in a single RADIUS database. RADIUS servers can proxy requests to remote servers for each.
realm-type [prefix|suffix]	Configures the realm-type used for NAI authentication • prefix – Sets the realm prefix. For example, in the realm name 'AC\JohnTalbot', the prefix is 'AC' and the user name 'JohnTalbot'. • suffix – Sets the realm suffix. For example, in the realm name 'JohnTalbot@AC.org' the suffix is 'AC.org' and the user name is 'JohnTalbot'.
realm <REALM-NAME>	Sets the realm information used for RADIUS authentication. The realm name should not exceed 50 characters. When the wireless controller or access point's RADIUS server receives a request for a user name the server references a table of usernames. If the user name is known, the server proxies the request to the RADIUS server. • <REALM-NAME> – Sets the realm used for authentication. This value is matched against the user name provided for RADIUS authentication. Example: Prefix - AC\JohnTalbot Suffix - JohnTalbot@AC.org
strip	Optional. Indicates the realm name must be stripped from the user name before sending it to the RADIUS server for authentication. For example, if the complete username is 'AC\JohnTalbot', then with the *strip* parameter enabled, only the 'JohnTalbot' part of the complete username is sent for authentication.

	`authentication server <1-6> onboard [controller|self]`
server <1-6>	Configures a RADIUS authentication server. Up to 6 RADIUS servers can be configured. • <1-6> – Specify the RADIUS server index from 1 - 6.
onboard [controller|self]	Selects the onboard RADIUS server for authentication instead of an external host • controller – Configures the wireless controller, to which the AP is adopted, as the onboard wireless controller • self – Configures the onboard server on the device (AP or wireless controller) where the client is associated as the onboard wireless controller

	`authentication server <1-6> proxy-mode [none|through-controller|through-mint-host <HOSTNAME/MINT-ID>| through-rf-domain-manager]`
server <1-6>	Configures a RADIUS authentication server. Up to 6 RADIUS servers can be configured. • <1-6> – Sets the RADIUS server index between 1 - 6
proxy-mode [none| through-controller| through-mint-host <HOSTNAME/MINT-ID>| through-rf-domain-manager]	Configures the mode for proxying a request • none – Proxying is not done. The packets are sent directly using the IP address of the device. • through-controller – Traffic is proxied through the wireless controller configuring this device • through-mint-host <HOSTNAME/MINT-ID> – Traffic is proxied through a neighboring MiNT device. Provide the device's hostname or MiNT ID. • through-rf-domain-manager – Traffic is proxied through the local RF Domain manager

`authentication server <1-6> retry-timeout-factor <50-200>`

server <1-6>	Configures a RADIUS authentication server. Up to 6 RADIUS servers can be configured. • <1-6> – Specify the RADIUS server index from 1 - 6.
retry-timeout-factor <50-200>	Configures the scaling of timeouts between two consecutive RADIUS authentication retries • <50-200> – Specify the scaling factor from 50 - 200. A value of 100 indicates the interval between two consecutive retires remains the same irrespective of the number of retries. A value lesser than 100 indicates the interval between two consecutive retries reduces with each successive retry. A value greater than 100 indicates the interval between two consecutive retries increases with each successive retry.

`authentication server <1-6> timeout <1-60> {attempts <1-10>}`

server <1-6>	Configures a RADIUS authentication server. Up to 6 RADIUS servers can be configured. • <1-6> – Specify the RADIUS server index from 1 - 6.
timeout <1-60>	Configures the timeout, in seconds, for each request sent to the RADIUS server. This is the time allowed to elapse before another request is sent to the RADIUS server. If a response is received from the RADIUS server within this time, no retry is attempted. • <1-60> – Specify a value from 1 - 60 seconds. The default is 3 seconds.
attempts <1-10>	Optional. Indicates the number of retry attempts to make before giving up • <1-10> – Specify a value from 1 -10. The default is 3.

Example

```
rfs7000-37FABE(config-aaa-policy-test)#authentication server 5 host
172.16.10.10 secret example port 1009

rfs7000-37FABE(config-aaa-policy-test)#authentication server 5 timeout 10
attempts 3

rfs7000-37FABE(config-aaa-policy-test)#authentication protocol chap

rfs7000-37FABE(config-aaa-policy-test)#show context
aaa-policy test
 authentication server 5 host 172.16.10.10 secret 0 example port 1009
 authentication server 5 timeout 10
 accounting server 2 host 172.16.10.10 secret 0 example port 1
 accounting server 2 timeout 2 attempts 2
 authentication protocol chap
 accounting interim interval 65
 accounting server preference auth-server-number
 attribute framed-mtu 110
rfs7000-37FABE(config-aaa-policy-test)#
```

Related Commands:

no	Resets authentication parameters on this AAA policy

health-check

aaa-policy

An AAA server could go offline. When a server goes offline, it is marked as *down*. This command configures the interval after which a server marked as *down* is checked to see if it has come back online and is reachable.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
health-check interval <60-86400>
```

Parameters

```
health-check interval <60-86400>
```

interval <60-86400>	Configures an interval (in seconds) after which a down server is checked to see if it is reachable again • <60-86400> – Specify a value from 60 - 86400 seconds.

Example

```
rfs7000-37FABE(config-aaa-policy-test)#health-check interval 4000

rfs7000-37FABE(config-aaa-policy-test)#show context
aaa-policy test
 authentication server 5 host 172.16.10.10 secret 0 example port 1009
 authentication server 5 timeout 10
 accounting server 2 host 172.16.10.10 secret 0 example port 1
 accounting server 2 timeout 2 attempts 2
 authentication protocol chap
 accounting interim interval 65
 accounting server preference auth-server-number
 health-check interval 4000
 attribute framed-mtu 110
rfs7000-37FABE(config-aaa-policy-test)#
```

Related Commands:

no	Resets the health-check interval for AAA servers

mac-address-format

aaa-policy

Configures the format MAC addresses are filled in RADIUS request frames

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
mac-address-format [middle-hyphen|no-delim|pair-colon|pair-hyphen|quad-dot]
mac-address-format [middle-hyphen|no-delim|pair-colon|pair-hyphen|quad-dot]
           case [lower|upper] attributes [all|username-password]
```

Parameters]

```
mac-address-format [middle-hyphen|no-delim|pair-colon|pair-hyphen|quad-dot]
case [lower|upper] attributes [all|username-password]
```

middle-hyphen	Configures the MAC address format as AABBCC-DDEEFF
no-delim	Configures the MAC address format as AABBCCDDEEFF (without delimitors)
pair-colon	Configures the MAC address format as AA:BB:CC:DD:EE:FF
pair-hyphen	Configures the MAC address display format as AA-BB-CC-DD-EE-FF (default setting)
quad-dot	Configures the MAC address display format as AABB.CCDD.EEFF
case [lower|upper]	Indicates the case the MAC address is formatted • lower – Indicates MAC address is in lower case. For example, aa:bb:cc:dd:ee:ff • upper – Indicates MAC address is in upper case. For example, AA:BB:CC:DD:EE:FF (default setting)
attributes [all| username-password]	Configures RADIUS attributes to which this MAC format is applicable • all – Applies to all attributes with MAC addresses such as username, password, calling-station-id, and called-station-id • username-password – Applies only to the username and password fields (default setting)

Example

```
rfs7000-37FABE(config-aaa-policy-test)#mac-address-format quad-dot case upper
attributes username-password

rfs7000-37FABE(config-aaa-policy-test)#show context
aaa-policy test
 authentication server 5 host 172.16.10.10 secret 0 example port 1009
 authentication server 5 timeout 10
 accounting server 2 host 172.16.10.10 secret 0 example port 1
 accounting server 2 timeout 2 attempts 2
 mac-address-format quad-dot case upper attributes username-password
 authentication protocol chap
 --More--
rfs7000-37FABE(config-aaa-policy-test)#
```

Related Commands:

no	Resets the MAC address format to default (pair-hyphen)

no

aaa-policy

Negates a AAA policy command or sets its default

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no [accounting|attribute|authentication|health-check|mac-address-format|
          proxy-attribute|server-pooling-mode|use]

no accounting interim interval
no accounting server preference
no accounting server <1-6> {dscp|nai-routing|proxy-mode|retry-timeout-factor|
          timeout}
no accounting type

no attribute [acct-delay-time|acct-multi-session-id|chargeable-user-identity|
          cisco-vsa
audit-session-id|framed-mtu|location-information|nas-ipv6-address|
          operator-name|service-type]

no authentication [eap|protocol|server]
no authentication eap wireless-client
[attempts|identity-request-retry-timeout|
          identity-request-timeout|retry-timeout-factor|timeout]
no authentication protocol
no authentication server <1-6>
{dscp|nac|nai-routing|proxy-mode|retry-timeout-factor|
          timeout}

no health-check interval

no mac-address-format

no proxy-attribute [nas-identifier|nas-ip-address]

no server-pooling-mode

no use nac-list
```

Parameters

`no accounting interim interval`

no accounting interim interval	Disables the periodic submission of accounting information

`no accounting server preference`

no accounting server preference	Resets the accounting server's preference to default

	`no accounting server <1-6> {dscp|nai-routing|proxy-mode|retry-timeout-factor|timeout}`
no accounting server <1-6>	Resets the RADIUS accounting server's (identified by its index number) settings
dscp	Optional. Resets the DSCP value for RADIUS accounting
nai-routing	Optional. Disables NAI forwarding requests
proxy-mode	Optional. Resets proxy mode to the default of "no proxying"
retry-timeout-factor	Optional. Resets retry timeout to its default of 100
timeout	Optional. Resets access parameters, such as timeout values and retry attempts to their default

	`no accounting type`
no accounting type	Resets the type of RADIUS accounting packets generated, to its default (start/stop)

	`no attribute [acct-delay-time|acct-multi-session-id|chargeable-user-identity|cisco-vsa audit-session-id|framed-mtu|location-information|nas-ipv6-address|operator-name| service-type]`
no attribute acct-delay-time	Disables support for accounting-delay-time attribute in accounting requests
no attribute acct-multi-session-id	Disables support for accounting-multi-session-id attribute
no attribute chargeable-user-identity	Disables support for chargeable-user-identity attribute
no attribute cisco-vsa audit-session-id	Removes the configured CISCO VSA audit session ID
no attribute framed-mtu	Resets Framed-MTU RADIUS server attribute in access and accounting requests
no attribute location-information	Disables support for RFC5580 location information attribute
no attribute nas-ipv6-address	Disables support for the NAS IPv6 address attribute
no attribute service-type	Disables support for the service-type (6) attribute

	`no authentication eap wireless-client [attempts|identity-request-timeout|retry-timeout-factor|timeout]`
no authentication eap wireless-client	Resets EAP parameters for wireless clients
attempts	Resets the number of times a RADIUS request is sent to a wireless client to default (3)
identity-request-retry-timeout	Resets the interval after which an EAP-identity request to the wireless client is retried
identity-request-timeout	Resets EAP identity request timeout to its default
retry-timeout-factor	Resets EAP retry timeout to its default of 100
timeout	Resets EAP timeout to its default

	`no authentication protocol`
authentication protocol	Resets the authentication protocol used for non-EAP authentication to its default (PAP authentication)

	`no authentication server <1-6> {dscp|nac|nai-routing|proxy-mode|retry-timeout-factor|timeout}`
no authentication server <1-6>	Resets the RADIUS authentication server's (identified by its index number) settings
dscp	Optional. Resets the DSCP value for RADIUS authentication
nac	Optional. Disables NAC on the selected RADIUS authentication server
nai-routing	Optional. Disables NAI forwarding requests
proxy-mode	Optional. Resets proxy mode to the default of "no proxying"
retry-timeout-factor	Optional. Resets retry timeout to its default of 100
timeout	Optional. Resets all access parameters, such as timeout and retry attempts to their default
	`no health-check interval`
no health-check interval	Resets all RADIUS servers' health check interval to its default
	`no mac-address-format`
no mac-address format	Resets the MAC address format used in RADIUS request frames
	`no proxy-attribute [nas-identifier|nas-ip-address]`
no proxy-attribute [nas-identifier| nas-ip-address]	Resets RADIUS attribute behavior when proxying through a controller or RF Domain manager
	`no server-pooling-mode`
no server-pooling-mode	Resets the mode used to select a AAA server from a pool of configured servers
	`no use nac-list`
no use nac-list	Detaches the current NAC list from this AAA policy

Example

```
The following example shows the AAA policy 'test' settings before the 'no'
commands are executed:

rfs7000-37FABE(config-aaa-policy-test)#show context
aaa-policy test
 authentication server 5 host 172.16.10.10 secret 0 example port 1009
 authentication server 5 timeout 10
 accounting server 2 host 172.16.10.10 secret 0 example port 1
 accounting server 2 timeout 2 attempts 2
 mac-address-format quad-dot case upper attributes username-password
 authentication protocol chap
 accounting interim interval 65
 accounting server preference auth-server-number
 health-check interval 4000
 attribute framed-mtu 110
rfs7000-37FABE(config-aaa-policy-test)#

rfs7000-37FABE(config-aaa-policy-test)#no accounting server 2 timeout 2
rfs7000-37FABE(config-aaa-policy-test)#no accounting interim interval
rfs7000-37FABE(config-aaa-policy-test)#no health-check interval
rfs7000-37FABE(config-aaa-policy-test)#no attribute framed-mtu
rfs7000-37FABE(config-aaa-policy-test)#no authentication protocol
```

```
The following example shows the AAA policy 'test' settings after the 'no'
commands are executed:

rfs7000-37FABE(config-aaa-policy-test)#show context
aaa-policy test
 authentication server 5 host 172.16.10.10 secret 0 example port 1009
 authentication server 5 timeout 10
 accounting server 2 host 172.16.10.10 secret 0 example port 1
 mac-address-format quad-dot case upper attributes username-password
 accounting server preference auth-server-number
 health-check interval 4000
rfs7000-37FABE(config-aaa-policy-test)#
```

Related Commands:

accounting	Configures RADIUS accounting parameters
attribute	Configures RADIUS Framed-MTU attribute used in access and accounting requests.
authentication	Configures RADIUS authentication parameters
health-check	Configures health-check parameters
mac-address-format	Configures the MAC address format used in RADIUS packets
proxy-attribute	Configures RADIUS server's attribute behavior when proxying through a wireless controller or a RF Domain Manager
server-pooling-mode	Configures the RADIUS server pooling mode
use	Permits the use of NAC access lists

proxy-attribute

aaa-policy

Configures RADIUS server's attribute behavior when proxying through a wireless controller or a RF Domain Manager

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
proxy-attribute [nas-identifier|nas-ip-address]
proxy-attribute [nas-identifier [originator|proxier]|nas-ip-address
[none|proxier]]
```

Parameters

```
proxy-attribute [nas-identifier [originator|proxier]|nas-ip-address
[none|proxier]]
```

nas-identifier [originator|proxier]	Uses NAS identifier • originator – Configures the NAS identifier as the originator of the RADIUS request. The originator could be an AP, or a wireless controller with radio. • proxier – Configures the proxying device as the NAS identifier. The device could be a controller or a RF Domain manager.
nas-ip-address [none|proxier]	Uses NAS IP address • none – NAS IP address attribute is not filled • proxier – NAS IP address is filled by the proxying device.The device could be a controller or a RF Domain manager.

Example

```
rfs7000-37FABE(config-aaa-policy-test)#proxy-attribute nas-ip-address proxier

rfs7000-37FABE(config-aaa-policy-test)#proxy-attribute nas-identifier
originator
```

Related Commands:

no	Resets RADIUS server's proxying attributes

server-pooling-mode

aaa-policy

Configures the server selection method from a pool of AAA servers. The available methods are *failover* and *load-balance*.

In the failover scenario, when a configured AAA server goes down, the server with the next higher index takes over for the failed server.

In the load-balance scenario, when a configured AAA server goes down, the remaining servers distribute the load amongst themselves.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
server-pooling-mode [failover|load-balance]
```

Parameters

```
server-pooling-mode [failover|load-balance]
```

failover	Sets the pooling mode to failover. This is the default setting. When a configured AAA server fails, the server with the next higher index takes over the failed server's load.
load-balance	Sets the pooling mode to load balancing When a configured AAA server fails, all servers in the pool share the failed server's load transmitting requests in a round-robin fashion.

Example

```
rfs7000-37FABE(config-aaa-policy-test)#server-pooling-mode load-balance

rfs7000-37FABE(config-aaa-policy-test)#show context
aaa-policy test
 authentication server 5 host 172.16.10.10 secret 0 example port 1009
 authentication server 5 timeout 10
 accounting server 2 host 172.16.10.10 secret 0 example port 1
 server-pooling-mode load-balance
 mac-address-format quad-dot case upper attributes username-password
 accounting server preference auth-server-number
 health-check interval 4000
rfs7000-37FABE(config-aaa-policy-test)#
```

Related Commands:

no	Resets the method of selecting a server, from the pool of configured AAA servers

use

aaa-policy

Associates a *Network Access Control* (NAC) with this AAA policy. This allows only the set of configured devices to use the configured AAA servers.

For more information on creating a NAC list, see *nac-list*.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
use nac-list <NAC-LIST-NAME>
```

Parameters

```
use nac-list <NAC-LIST-NAME>
```

nac-list <NAC-LIST-NAME>	Associates a NAC list with this AAA policy • <NAC-LIST-NAME> – Specify the NAC list name (should be existing and configured).

Example

```
rfs7000-37FABE(config-aaa-policy-test)#use nac-list test1

rfs7000-37FABE(config-aaa-policy-test)#show context
aaa-policy test
 authentication server 5 host 172.16.10.10 secret 0 example port 1009
 authentication server 5 timeout 10
 accounting server 2 host 172.16.10.10 secret 0 example port 1
 server-pooling-mode load-balance
 mac-address-format quad-dot case upper attributes username-password
 accounting server preference auth-server-number
 health-check interval 4000
 use nac-list test1
rfs7000-37FABE(config-aaa-policy-test)#
```

Related Commands:

no	Resets set values or disables commands
nac-list	Creates a NAC list

Chapter

AUTO-PROVISIONING-POLICY 9

This chapter summarizes the auto provisioning policy commands in the CLI command structure.

Wireless devices can adopt and manage other wireless devices. For example, a wireless controller can adopt multiple access points. When a device is adopted, the device configuration is provisioned by the adopting device. Since multiple configuration policies are supported, an adopting device uses auto provisioning policies to determine which configuration policies are applied to an adoptee based on its properties. For example, a configuration policy could be assigned based on MAC address, IP address, CDP snoop strings, etc.

Auto provisioning or adoption is the process by which an access point discovers controllers in the network, identifies the most desirable controller, associates with the identified controller, and optionally obtains an image upgrade, obtains its configuration and considers itself provisioned.

At adoption, an access point solicits and receives multiple adoption responses from controllers available on the network. These adoption responses contain loading policy information the access point uses to select the optimum controller for adoption. An auto-provisioning policy maps a new AP to a profile and RF Domain based on various parameters related to the AP and where it is connected. By default a new AP will be mapped to the default profile and default RF Domain. Modify existing
auto-provisioning policies or create a new one as needed to meet the configuration requirements of a device.

An auto-provisioning policy enables an administrator to define rules for the supported Brocade access points capable of being adopted by a controller. The policy determines which configuration policies are applied to an adoptee based on its properties. For example, a configuration policy could be assigned based on MAC address, IP address, *CISCO Discovery Protocol* (CDP) snoop strings, etc. Once created an auto provisioning policy can be used in profiles or device configuration objects. The policy contains a set of rules (ordered by precedence) that either deny or allow adoption based on potential adoptee properties and a catch-all variable that determines if the adoption should be allowed when none of the rules is matched. All rules (both deny and allow) are evaluated sequentially starting with the rule with the lowest precedence. The evaluation stops as soon as a rule has been matched, no attempt is made to find a better match further down in the set.

For example,

```
rule #1 adopt br7131 10 profile default vlan 10
rule #2 adopt br650  20 profile default vlan 20
rule #3 adopt br7131 30 profile default serial-number
rule #4 adopt br7131 40 p d mac aa bb
```

Brocade Mobility 7131 Access Point L2 adoption, VLAN 10 - will use rule #1

Brocade Mobility 7131 Access Point L2 adoption, VLAN 20 - will not use rule #2 (wrong type), may use rule #3 if the serial number matched, or rule #4

If aa<= MAC <= bb, or else default.

With the implementation of the *hierarchically managed* (HM) network, the auto-provisioning policy has been modified to enable controllers to adopt other controllers in addition to access points.

The new Mobility HM network defines a three-tier structure, consisting of multiple wireless sites managed by a single *Network Operations Center* (NOC) controller, The NOC controller constitutes the first and the site controllers constitute the second tier of the hierarchy. The site controllers in turn adopt and manage access points that form the third tier of the hierarchy.

All adopted devices (access points and second-level controllers) are referred to as the 'adoptee'. The adopting devices are the 'adopters'.

A controller cannot be configured as an adoptee and an adopter simultaneously. In other words, a controller can either be an adopter (adopts another controller) or an adoptee (is adopted by another controller). Therefore, a site controller, which has been adopted by a NOC controller, cannot adopt another controller. But it can adopt access points. For more information on HM network, see *device-upgrade*.

A controller should be configured to specify the device types (APs and/or controllers) that it can adopt. For more information on configuring the adopted-device types for a controller, see *controller*.

NOTE
The adoption capabilities of a controller depends on:
Whether the controller is deployed at the NOC or site
- A NOC controller can adopt site controllers and access points
- A site controller can adopt access points only
- The controller device type, which determines the number and type of devices it can adopt

The NOC controller can adopt a site controller with a capacity equal to or lower than its own. The following defines the adoption capabilities of the various controller devices:

- Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point and AP82XX (when configured as a controller) – Can adopt Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Brocade Mobility RFS4000 – Can adopt another Brocade Mobility RFS4000 only
- Brocade Mobility RFS6000 and Brocade Mobility RFS7000 – Can adopt Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Use the (config) instance to configure an auto-provisioning policy. To navigate to the auto-provisioning-policy configuration instance, use the following command:

```
<DEVICE>(config)#auto-provisioning-policy <POLICY-NAME>

rfs7000-37FABE(config)#auto-provisioning-policy test
rfs7000-37FABE(config-auto-provisioning-policy-test)#?
Auto-Provisioning Policy Mode commands:
  adopt             Add rule for device adoption
  default-adoption  Adopt devices even when no matching rules are found.
                    Assign default profile and default rf-domain
  deny              Add rule to deny device adoption
  no                Negate a command or set its defaults
  redirect          Add rule to redirect device adoption
  upgrade           Add rule for device upgrade

  clrscr            Clears the display screen
  commit            Commit all changes made in this session
  do                Run commands from Exec mode
  end               End current mode and change to EXEC mode
  exit              End current mode and down to previous mode
  help              Description of the interactive help system
  revert            Revert changes
```

```
  service          Service Commands
  show             Show running system information
  write            Write running configuration to memory or terminal

rfs7000-37FABE(config-auto-provisioning-policy-test)#
```

auto-provisioning-policy

Table 7 summarizes auto provisioning policy configuration commands.

TABLE 7 Auto-Provisioning-Policy-Config Commands

Command	Description	Reference
adopt	Adds a permit adoption rule	page 855
default-adoption	Adopts devices even when no matching rules are found. Assigns default profile and default RF Domain	page 861
deny	Adds a deny adoption rule	page 861
redirect	Adds a rule redirecting device adoption to a specified controller within the system	page 864
upgrade	Adds a device upgrade rue to this auto provisioning policy	page 867
no	Negates a command or reverts settings to their default	page 870
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 387
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

adopt

auto-provisioning-policy

Adds device adoption rules

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
adopt
[ap621|ap622|br650|br6511|ap6521|br1220|ap6532|ap6562|br71xx|br81xx|ap82xx|
          rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx9000]

adopt
[ap621|ap622|br650|br6511|ap6521|br1220|ap6532|ap6562|br71xx|br81xx|ap82xx|
          rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx9000] precedence <1-10000>
          [profile|rf-domain]

adopt
[ap621|ap622|br650|br6511|ap6521|br1220|ap6532|ap6562|br71xx|br81xx|ap82xx|
          rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx9000] precedence <1-10000>
          [profile <DEVICE-PROFILE-NAME>|rf-domain <RF-DOMAIN-NAME>]

[any|cdp-match|dhcp-option|fqdn|ip|lldp-match|mac|model-number|rf-domain|
          serial-number|vlan]

adopt
[ap621|ap622|br650|br6511|ap6521|br1220|ap6532|ap6562|br71xx|br81xx|ap82xx|
          rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx9000] precedence <1-10000>
          [profile <DEVICE-PROFILE-NAME>|rf-domain <RF-DOMAIN-NAME>] any

adopt
[ap621|ap622|br650|br6511|ap6521|br1220|ap6532|ap6562|br71xx|br81xx|ap82xx|
          rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx9000] precedence <1-10000>
          [profile <DEVICE-PROFILE-NAME>|rf-domain <RF-DOMAIN-NAME>]
          [cdp-match <LOCATION-SUBSTRING>|dhcp-option <DHCP-OPTION>|fqdn
<FQDN>|
          ip [<START-IP> <END-IP>|<IP/MASK>]|lldp-match <LLDP-STRING>|
          mac <START-MAC> {<END-MAC>}|model-number <MODEL-NUMBER>|
          serial-number <SERIAL-NUMBER>|rf-domain <RF-DOMAIN-NAME>|vlan
<VLAN-ID>]
```

Parameters

```
adopt
[ap621|ap622|br650|br6511|ap6521|br1220|ap6532|ap6562|br71xx|br81xx|ap82xx|
rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx9000] precedence <1-10000>
[profile <DEVICE-PROFILE-NAME>|rf-domain <RF-DOMAIN-NAME>] any
```

adopt	Adds an adopt device rule. The rule applies to the selected device types. Specify the device type and assign a precedence to the rule. The different device types are: • Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point • Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000 • Service Platforms —Brocade Mobility RFS9510
precedence <1-10000>	Sets the rule precedence from 1 - 10000. A rule with a lower value has a higher precedence.

profile <DEVICE-PROFILE-NAME>	Sets the device profile for this provisioning policy. The selected device profile must be appropriate for the device being provisioned. For example, use an Brocade Mobility 650 Access Point device profile for an Brocade Mobility 650 Access Point. Using an inappropriate device profile can result in unpredictable results. Provide a device profile name. Provide a device profile name. Or a template with appropriate substitution tokens, such as 'campus-$MODEL[1:6]', 'FQDN[1:4]-indoor' Available tokens: $FQDN - references FQDN of adopting device $CDP - references CDP Device Id of wired switch to which adopting device is connected $LLDP - references LLDP System Name of wired switch to which adopting device is connected $DHCP - references DHCP Option Value received by the adopting device $SN - references SERIAL NUMBER of adopting device $MODEL - references MODEL NUMBER of adopting device $DNS-SUFFIX - references FQDN excluding the hostname of the adopting device
rf-domain <RF-DOMAIN-NAME>	Sets the RF Domain for this auto provisioning policy. The provisioning policy is only applicable to devices that try to become a part of the specified RF Domain. Provide the full RF Domain name OR use a string alias to identify the RF Domain. Provide the full RF Domain name or an alias. Or a template with appropriate substitution tokens, such as '$CDP[1:7]', '$DNS-SUFFIX[1:5]' Available tokens: $FQDN - references FQDN of adopting device $CDP - references CDP Device Id of wired switch to which adopting device is connected $LLDP - references LLDP System Name of wired switch to which adopting device is connected $DHCP - references DHCP Option Value received by the adopting device $SN - references SERIAL NUMBER of adopting device $MODEL - references MODEL NUMBER of adopting device $DNS-SUFFIX - references FQDN excluding the hostname of the adopting device Available built-in aliases: $_builtin_rf-domain - rf-domain of adopting device Use the built-in string alias or a user-defined string alias. String aliases allow you to configure APs in the same RF Domain as the adopting controller. A string alias maps a name to an arbitrary string value, for example, ‘alias string $DOMAIN test.brocade.com’. In this example, the string-alias *$DOMAIN* is mapped to the string: *test.brocade.com*. For more information, see *alias*.
any	Indicates any device. Any device seeking adoption is adopted.

```
adopt
[ap621|ap622|br650|br6511|ap6521|br1220|ap6532|ap6562|br71xx|br81xx|ap82xx|
rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx9000] precedence <1-10000>
[profile <DEVICE-PROFILE-NAME>|rf-domain <RF-DOMAIN-NAME>]
[cdp-match <LOCATION-SUBSTRING>|dhcp-option <DHCP-OPTION>|fqdn <FQDN>|
```

```
ip [<START-IP> <END-IP>|<IP/MASK>]|lldp-match <LLDP-STRING>|
mac <START-MAC> {<END-MAC>}|model-number <MODEL-NUMBER>|serial-number
<SERIAL-NUMBER>|
rf-domain <RF-DOMAIN-NAME>|vlan <VLAN-ID>]
```

adopt	Adds an adopt device rule. The rule applies to the selected device types. Specify the device type and assign a precedence to the rule. The different device types are: • Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point • Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000 • Service Platforms — Brocade Mobility RFS9510
precedence <1-10000>	Sets the rule precedence. A rule with a lower value has a higher precedence.
profile <DEVICE-PROFILE-NAME>	Sets the device profile for this provisioning policy. The selected device profile must be appropriate for the device being provisioned. For example, use an Brocade Mobility 650 Access Point device profile for an Brocade Mobility 650 Access Point. Using an inappropriate device profile can result in unpredictable results. Provide a device profile name. Or a template with appropriate substitution tokens, such as 'campus-$MODEL[1:6]', 'FQDN[1:4]-indoor' Available tokens: $FQDN - references FQDN of adopting device $CDP - references CDP Device Id of wired switch to which adopting device is connected $LLDP - references LLDP System Name of wired switch to which adopting device is connected $DHCP - references DHCP Option Value received by the adopting device $SN - references SERIAL NUMBER of adopting device $MODEL - references MODEL NUMBER of adopting device $DNS-SUFFIX - references FQDN excluding the hostname of the adopting device
rf-domain <RF-DOMAIN-NAME>	Sets the RF Domain for this auto provisioning policy. The provisioning policy is only applicable to devices that try to become a part of the specified RF Domain. Provide the full RF Domain name or an alias. Or a template with appropriate substitution tokens, such as '$CDP[1:7]', '$DNS-SUFFIX[1:5]' Available tokens: $FQDN - references FQDN of adopting device $CDP - references CDP Device Id of wired switch to which adopting device is connected $LLDP - references LLDP System Name of wired switch to which adopting device is connected $DHCP - references DHCP Option Value received by the adopting device $SN - references SERIAL NUMBER of adopting device $MODEL - references MODEL NUMBER of adopting device $DNS-SUFFIX - references FQDN excluding the hostname of the adopting device Available built-in aliases:$_builtin_rf-domain - rf-domain of adopting device Use the built-in string alias or a user-defined string alias. String aliases allow you to configure APs in the same RF Domain as the adopting controller. A string alias maps a name to an arbitrary string value, for example, 'alias string $DOMAIN test.brocade.com'. In this example, the string-alias *$DOMAIN* is mapped to the string: *test.brocade.com*. For more information, see *alias*.

cdp-match <LOCATION-SUBSTRING>	Matches a substring in a list of CDP snoop strings (case insensitive). For example, if an access point snooped 3 devices: controller1.example.com, controller2.example.com, and controller3.example.com, 'controller1', ‘example’, 'example.com', are examples of the substrings that will match. • <LOCATION-SUBSTRING> – Specify the value to match. Devices matching the specified value are adopted.
dhcp-option <DHCP-OPTION>	Matches the value found in DHCP vendor option 191 (case insensitive). DHCP vendor option 191 can be setup to communicate various configuration parameters to an AP. The value of the option in a string in the form of tag=value separated by a semicolon, for example 'tag1=value1;tag2=value2;tag3=value3'. The access point includes the value of tag 'rf-domain', if present. • <DHCP-OPTION> – Specify the DHCP option. Devices matching the specified value are adopted.
fqdn <FQDN>	Matches a substring to the *Fully Qualified Domain Name* (FQDN) of a device (case insensitive) FQDN is a domain name that specifies its exact location in the DNS hierarchy. It specifies all domain levels, including its top-level domain and the root domain. This parameter allows a device to adopt based on its FQDN value. • <FQDN> – Specify the FQDN. Devices matching the specified value are adopted.
ip [<START-IP> <END-IP>| <IP/MASK>]	Adopts a device if its IP address matches the specified IP address or is within the specified IP address range. Or if the device is a part of the specified subnet. • <START-IP> – Specify the first IP address in the range. • <END-IP> – Specify the last IP address in the range. • <IP/MASK> – Specify the IP subnet and mask to match against the device’s IP address.
lldp-match <LLDP-STRING>	Matches a substring in a list of *Link Layer Discovery Protocol* (LLDP) snoop strings (case insensitive). For example, if an access point snooped 3 devices: controller1.example.com, controller2.example.com, and controller3.example.com,'controller1', 'example', 'example.com', are examples of the substrings that will match. LLDP is a vendor neutral link layer protocol that advertises a network device’s identity, capabilities, and neighbors on a local area network. • <LLDP-STRING> – Specify the LLDP string. Devices matching the specified value are adopted.
mac <START-MAC> {<END-MAC>}	Adopts a device if its MAC address matches the specified MAC address or is within the specified MAC address range • <START-MAC> – Specify the first MAC address in the range. Provide this MAC address if you want to match for a single device. • <END-MAC> – Optional. Specify the last MAC address in the range.
model-number <MODEL-NUMBER>	Adopts a device if its model number matches <MODEL-NUMBER> • <MODEL-NUMBER> – Specify the model number.

rf-domain <RF-DOMAIN-NAME>	Adopts a device if its RF Domain matches <RF-DOMAIN-NAME> <RF-DOMAIN-NAME> – Specify the RF Domain name. You can use a string alias to specify a RF Domain. Provide the full RF Domain name or an alias. Or a template with appropriate substitution tokens, such as '$CDP[1:7]', '$DNS-SUFFIX[1:5]' Available tokens: $FQDN - references FQDN of adopting device $CDP - references CDP Device Id of wired switch to which adopting device is connected $LLDP - references LLDP System Name of wired switch to which adopting device is connected $DHCP - references DHCP Option Value received by the adopting device $SN - references SERIAL NUMBER of adopting device $MODEL - references MODEL NUMBER of adopting device $DNS-SUFFIX - references FQDN excluding the hostname of the adopting device Available built-in aliases: $_builtin_rf-domain - rf-domain of adopting device Use the built-in string alias or a user-defined string alias. String aliases allow you to configure APs in the same RF Domain as the adopting controller. A string alias maps a name to an arbitrary string value, for example, 'alias string $DOMAIN test.brocade.com'. In this example, the string-alias *$DOMAIN* is mapped to the string: *test.brocade.com*. For more information, see *alias*.
serial-number <SERIAL-NUMBER>	Adopts a device if its serial number matches <SERIAL-NUMBER> • <SERIAL-NUMBER> – Specify the serial number.
vlan <VLAN-ID>	Adopts a device if its VLAN matches <VLAN-ID> • <VLAN-ID> – Specify the VLAN ID.

Example

```
rfs4000-229D58(config-auto-provisioning-policy-test)#adopt br81xx precedence
1 profile default-br81xx vlan 1

rfs4000-229D58(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
 adopt br81xx precedence 1 profile default-br81xx vlan 1
rfs4000-229D58(config-auto-provisioning-policy-test)#

rfs4000-229D58(config-auto-provisioning-policy-test)#show wireless br
configured
-------------------------------------------------------------------------------
------------------
 IDX       NAME               MAC              PROFILE       RF-DOMAIN
ADOPTED-BY
-------------------------------------------------------------------------------
------------------
 1    br81xx-711728    B4-C7-99-71-17-28    default-br81xx    default
00-23-68-22-9D-58
 2   rfs4000-229D58   00-23-68-22-9D-58   default-rfs4000   default
-------------------------------------------------------------------------------
------------------
rfs4000-229D58(config-auto-provisioning-policy-test)#
```

Related Commands:

no	Removes an adopt rule

default-adoption

auto-provisioning-policy

Adopts devices, even when no matching rules are defined. Assigns a default profile and default RF Domain.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
default-adoption
```

Parameters

None

Example

```
rfs4000-229D58(config-auto-provisioning-policy-test)#default-adoption

rfs4000-229D58(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
 default-adoption
 adopt br81xx precedence 1 profile default-br81xx vlan 1
rfs4000-229D58(config-auto-provisioning-policy-test)#
```

Related Commands:

no	Disables adoption of devices when matching rules are not found

deny

auto-provisioning-policy

Defines a deny device adoption rule

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
deny
[ap621|ap622|br650|br6511|ap6521|br1220|ap6532|ap6562|br71xx|br81xx|ap82xx|
          rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx9000]

deny
[ap621|ap622|br650|br6511|ap6521|br1220|ap6532|ap6562|br71xx|br81xx|ap82xx|
          rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx9000] precedence <1-10000>

[any|cdp-match|dhcp-option|fqdn|ip|lldp-match|mac|model-number|serial-number|
vlan]

deny
[ap621|ap622|br650|br6511|ap6521|br1220|ap6532|ap6562|br71xx|br81xx|ap82xx|
          rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx9000] precedence <1-10000>
any

deny
[ap621|ap622|br650|br6511|ap6521|br1220|ap6532|ap6562|br71xx|br81xx|ap82xx|
          rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx9000] precedence <1-10000>
          [cdp-match <LOCATION-SUBSTRING>|dhcp-option <DHCP-OPTION>|fqdn
<FQDN>|
          ip [<START-IP> <END-IP>|<IP/MASK>]|lldp-match <LLDP-STRING>|
          mac <START-MAC> {<END-MAC>}|model-number <MODEL-NUMBER>|
          serial-number <SERIAL-NUMBER>|vlan <VLAN-ID>]
```

Parameters

```
deny
[ap621|ap622|br650|br6511|ap6521|br1220|ap6532|ap6562|br71xx|br81xx|ap82xx|
rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx9000] precedence <1-10000> any
```

deny	Adds a deny adoption rule. The rule applies to the selected device types. Specify the device type and assign a precedence to the rule. The different device types are: • Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point • Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000 • Service Platforms — Brocade Mobility RFS9510
precedence <1-10000>	Sets the rule precedence. A rule with a lower value has a higher precedence.
any	Indicates any device. Any device seeking adoption is denied adoption.

```
deny
[ap621|ap622|br650|br6511|ap6521|br1220|ap6532|ap6562|br71xx|br81xx|ap82xx|
rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx9000] precedence <1-1000> [cdp-match
<LOCATION-SUBSTRING>|dhcp-option <DHCP-OPTION>|fqdn <FQDN>|ip [<START-IP>
<END-IP>|<IP/MASK>]|
lldp-match <LLDP-STRING>|mac <START-MAC> {<END-MAC>}|model-number
<MODEL-NUMBER>|serial-number <SERIAL-NUMBER>|vlan <VLAN-ID>]
```

deny	Adds a deny adoption rule. The rule applies to the selected device types. Specify the device type and assign a precedence to the rule. The different device types are: • Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point • Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000 • Service Platforms — Brocade Mobility RFS9510
precedence <1-10000>	Sets the rule precedence. A rule with a lower value has a higher precedence. After specifying the rule precedence, specify the match criteria. Devices matching the specified criteria are denied adoption.
cdp-match <LOCATION-SUBSTRING>	Matches a substring in a list of CDP snoop strings (case insensitive). For example, if an access point snooped 3 devices: controller1.example.com, controller2.example.com and controller3.example.com, 'controller1', ‘example’, 'example.com', are examples of the substrings that will match. • <LOCATION-SUBSTRING> – Specify the value to match. Devices matching the specified value are denied adoption.
dhcp-option <DHCP-OPTION>	Matches the value found in DHCP vendor option 191 (case insensitive). DHCP vendor option 191 can be setup to communicate various configuration parameters to an AP. The value of the option in a string in the form of tag=value separated by a semicolon, for example 'tag1=value1;tag2=value2;tag3=value3'. The access point includes the value of tag 'rf-domain', if present. • <DHCP-OPTION> – Specify the DHCP option value to match. Devices matching the specified value are denied adoption.
fqdn <FQDN>	Matches a substring to the FQDN of a device (case insensitive) FQDN is a domain name that specifies its exact location in the DNS hierarchy. It specifies all domain levels, including its top-level domain and the root domain. • <FQDN> – Specify the FQDN. Devices matching the specified value are denied adoption.
ip [<START-IP> <END-IP>|<IP/MASK>]	Denies adoption if a device's IP address matches the specified IP address or is within the specified IP address range • <START-IP> – Specify the first IP address in the range. • <END-IP> – Specify the last IP address in the range. • <IP/MASK> – Specify the IP subnet and mask to match against the device’s IP address.
lldp-match <LLDP-STRING>	Matches a substring in a list of LLDP snoop strings (case insensitive). For example, if an access point snooped 3 devices: controller1.example.com, controller2.example.com and controller3.example.com,'controller1', 'example', 'example.com', are examples of the substrings that will match. LLDP is a vendor neutral link layer protocol used to advertise a network device’s identity, capabilities, and neighbors on a local area network. • <LLDP-STRING> – Specify the LLDP string. Devices matching the specified values are denied adoption.
mac <START-MAC> {<END-MAC>}	Denies adoption if a device's MAC address matches the specified MAC address or is within the specified MAC address range • <START-MAC> – Specify the first MAC address in the range. Provide this MAC address if you want to match for a single device. • <END-MAC> – Optional. Specify the last MAC address in the range.
model-number <MODEL-NUMBER>	Denies adoption if a device’s model number matches <MODEL-NUMBER> • <MODEL-NUMBER> – Specify the model number.

serial-number <SERIAL-NUMBER>	Denies adoption if a device's serial number matches <SERIAL-NUMBER> • <SERIAL-NUMBER> – Specify the serial number.
vlan <VLAN-ID>	Denies adoption if a device's VLAN matches <VLAN-ID> • <VLAN-ID> – Specify the VLAN ID.

Example

```
rfs4000-229D58(config-auto-provisioning-policy-test)#deny br71xx precedence 2
model-number AP7131N

rfs4000-229D58(config-auto-provisioning-policy-test)#deny br71xx precedence 3
ip 192.168.13.23 192.168.13.23

rfs4000-229D58(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
 adopt br81xx precedence 1 profile default-br81xx vlan 1
 deny br71xx precedence 2 model-number AP7131N
 deny br71xx precedence 3 ip 192.168.13.23 192.168.13.23
rfs4000-229D58(config-auto-provisioning-policy-test)#
```

Related Commands:

no	Removes a deny adoption rule

redirect

auto-provisioning-policy

Adds a rule redirecting device adoption to another controller within the system. Devices seeking adoption are redirected to a specified controller based on the redirection parameters specified.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
redirect
[ap621|ap622|br650|br6511|ap6521|br1220|ap6532|ap6562|br71xx|br81xx|ap82xx|
          rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx9000]

redirect
[ap621|ap622|br650|br6511|ap6521|br1220|ap6532|ap6562|br71xx|br81xx|ap82xx|
          rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx9000] precedence <1-10000>
          controller [<CONTROLLER-IP>|<CONTROLLER-HOSTNAME>]
[any|cdp-match|dhcp-option|
          fqdn|ip|lldp-match|mac|model-number|serial-number|vlan]
```

```
redirect
[ap621|ap622|br650|br6511|ap6521|br1220|ap6532|ap6562|br71xx|br81xx|ap82xx|
          rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx9000] precedence <1-10000>
          controller [<CONTROLLER-IP>|<CONTROLLER-HOSTNAME>] any

redirect
[ap621|ap622|br650|br6511|ap6521|br1220|ap6532|ap6562|br71xx|br81xx|ap82xx|
          rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx9000] precedence <1-10000>
          controller [<CONTROLLER-IP>|<CONTROLLER-HOSTNAME>] [cdp-match
<LOCATION-SUBSTRING>|
          dhcp-option <DHCP-OPTION>|fqdn <FQDN>|ip [<START-IP>
<END-IP>|<IP/MASK>]|
          lldp-match <LLDP-STRING>|mac <START-MAC> {<END-MAC>}|model-number
<MODEL-NUMBER>|
          serial-number <SERIAL-NUMBER>|vlan <VLAN-ID>]
```

Parameters

```
redirect [ap621|ap622|br650|br6511|ap6521|br1220|ap6532|ap6562|br71xx|br81xx|
ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx9000] precedence <1-10000>
       controller [<CONTROLLER-IP>|<CONTROLLER-HOSTNAME>] any
```

redirect	Adds a redirect adoption rule. The rule applies to the device type selected. Specify the device type and assign a precedence to the rule. The different device types are: • Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point • Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000 • Service Platforms — Brocade Mobility RFS9510 An adoptee controller, such as Brocade Mobility RFS4000, Brocade Mobility RFS6000, and Brocade Mobility RFS7000, can be redirected to another controller (configured to adopt controllers) with a capacity equal to or higher than its own. For more information, see *controller*.
precedence <1-10000>	Sets the rule precedence. Rules with lower values get precedence over rules with higher values.
controller [<CONTROLLER-IP>| <CONTROLLER-HOSTNAME>]	Configures the controller to which the adopting devices are redirected. Specify the controller's IP address or hostname. • <CONTROLLER-IP> – Specifies the controller's IP address • <CONTROLLER-HOSTNAME> – Specifies the controller's hostname
any	Indicates any device. Any device seeking adoption is redirected.

```
deny
[ap621|ap622|br650|br6511|ap6521|br1220|ap6532|ap6562|br71xx|br81xx|ap82xx|
rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx9000] precedence <1-1000> controller
[<CONTROLLER-IP>|<CONTROLLER-HOSTNAME>] [cdp-match
<LOCATION-SUBSTRING>|dhcp-option <DHCP-OPTION>|fqdn <FQDN>|ip [<START-IP>
```

```
<END-IP>|<IP/MASK>]|lldp-match <LLDP-STRING>|
mac <START-MAC> {<END-MAC>}|model-number <MODEL-NUMBER>|serial-number
<SERIAL-NUMBER>|
vlan <VLAN-ID>]
```

redirect	Adds a redirect adoption rule. The rule applies to the device type selected. Specify the device type and assign a precedence to the rule. The different device type options are: • Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point • Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000 • Service Platforms — Brocade Mobility RFS9510 An adoptee controller, such as Brocade Mobility RFS4000, Brocade Mobility RFS6000, and Brocade Mobility RFS7000, can be redirected to another controller (configured to adopt controllers) with a capacity equal to or higher than its own. For more information, see *controller*.
precedence <1-10000>	Sets the rule precedence. Rules with lower values get precedence over rules with higher values.
controller [<CONTROLLER-IP>| <CONTROLLER-HOSTNAME >]	Configures the controller to which the adopting devices are redirected. Specify the controller's IP address or hostname. • <CONTROLLER-IP> – Specifies the controller's IP address • <CONTROLLER-HOSTNAME> – Specifies the controller's hostname After specifying the rule precedence and the controller, specify the match criteria.
cdp-match <LOCATION-SUBSTRING>	Configures the device location to match, based on CDP snoop strings • <LOCATION-SUBSTRING> – Specify the location. Devices matching the specified string are redirected.
dhcp-option <DHCP-OPTION>	Configures the DHCP options to match DHCP options identify the vendor and DHCP client functionalities. This information is used by the client to convey to the DHCP server that the client requires extra information in a DHCP response. • <DHCP-OPTION> – Specify the DHCP option value. Devices matching the specified value are redirected.
fqdn <FQDN>	Configures the FQDN to match FQDN is a domain name that specifies its exact location in the DNS hierarchy. It specifies all domain levels, including its top-level domain and the root domain. • <FQDN> – Specify the FQDN. Devices matching the specified value are redirected.
ip [<START-IP> <END-IP>|<IP/MASK>]	Configures a range of IP addresses and subnet address. Devices having IP addresses within the specified range or are part of the specified subnet are redirected. • <START-IP> – Specify the first IP address in the range. • <END-IP> – Specify the last IP address in the range. • <IP/MASK> – Specify the IP subnet and mask to match against the device's IP address.
lldp-match <LLDP-STRING>	Configures the device location to match, based on LLDP snoop strings LLDP is a vendor neutral link layer protocol used to advertise a network device's identity, capabilities, and neighbors on a local area network. • <LLDP-STRING> – Specify the location. Devices matching the specified string are redirected.
mac <START-MAC> {<END-MAC>}	Configures a single or a range of MAC addresses. Devices matching the specified values are redirected. • <START-MAC> – Specify the first MAC address in the range. Provide only this MAC address to filter a single device. • <END-MAC> – Optional. Specify the last MAC address in the range.
model-number <MODEL-NUMBER>	Configures the device model number • <MODEL-NUMBER> – Specify the model number. Devices matching the specified model number are redirected.

serial-number <SERIAL-NUMBER>	Configures the device's serial number • <SERIAL-NUMBER> – Specify the serial number. Devices matching the specified serial number are redirected.
vlan <VLAN-ID>	Configures the VLAN ID • <VLAN-ID> – Specify the VLAN ID. Devices assigned to the specified VLAN are redirected.

Example

```
rfs4000-229D58(config-auto-provisioning-policy-test)#redirect br81xx
precedence 4 controller 192.168.13.10 ip 192.168.13.25 192.168.13.25

rfs4000-229D58(config-auto-provisioning-policy-test)#redirect br81xx
precedence 5 controller 192.168.13.10 model-number AP-8132-66040-US

rfs4000-229D58(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
 default-adoption
 adopt br81xx precedence 1 profile default-br81xx vlan 1
 deny br71xx precedence 2 model-number AP7131N
 deny br71xx precedence 3 ip 192.168.13.23 192.168.13.23
 redirect br81xx precedence 4 controller 192.168.13.10 ip 192.168.13.25
192.168.13.25
 redirect br81xx precedence 5 controller 192.168.13.10 model-number
AP-8132-66040-US
rfs4000-229D58(config-auto-provisioning-policy-test)#
```

Related Commands:

no	Removes a redirect rule

upgrade

auto-provisioning-policy

Adds a device upgrade rule to this auto provisioning policy

When applied to a controller, the upgrade rule ensures adopted devices, of the specified type, are upgraded automatically.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
upgrade
[ap621|ap622|br650|br6511|ap6521|br1220|ap6532|ap6562|br71xx|br81xx|ap82xx|
          rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx9000]
```

```
upgrade
[ap621|ap622|br650|br6511|ap6521|br1220|ap6532|ap6562|br71xx|br81xx|ap82xx|
          rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx9000] precedence <1-10000>

[any|cdp-match|dhcp-option|fqdn|ip|lldp-match|mac|model-number|serial-number|
vlan]

upgrade
[ap621|ap622|br650|br6511|ap6521|br1220|ap6532|ap6562|br71xx|br81xx|ap82xx|
          rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx9000] precedence <1-10000>
any

upgrade
[ap621|ap622|br650|br6511|ap6521|br1220|ap6532|ap6562|br71xx|br81xx|ap82xx|
          rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx9000] precedence <1-10000>
          [cdp-match <LOCATION-SUBSTRING>|dhcp-option <DHCP-OPTION>|fqdn
<FQDN>|
          ip [<START-IP> <END-IP>|<IP/MASK>]|lldp-match <LLDP-STRING>|
          mac <START-MAC> {<END-MAC>}|model-number <MODEL-NUMBER>|
          serial-number <SERIAL-NUMBER>|vlan <VLAN-ID>]|lldp-match
<LLDP-STRING>|
          mac <STARTING-MAC> {<ENDING-MAC>}|model-number <MODEL-NUMBER>|
          serial-number <SERIAL-NUMBER>|vlan <VLAN-ID>]
```

Parameters

```
upgrade [ap621|ap622|br650|br6511|ap6521|br1220|ap6532|ap6562|br71xx|br81xx|
ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx9000] precedence <1-10000> any
```

upgrade	Adds a device upgrade rule. The rule applies to the device type selected. Specify the device type and assign a precedence to the rule. The different device types are: • Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point • Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000 • Service Platforms — Brocade Mobility RFS9510

precedence <1-10000>	Sets the rule precedence. Rules with lower values get precedence over rules with higher values.
any	Supported in the following platforms:Indicates any device. Any device, of the selected type, is upgraded. For example, if the device type selected is • Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point • Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000 • Service Platforms — , Brocade Mobility RFS9510 Supported in the following platforms:, any • Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point • Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000 • Service Platforms — , Brocade Mobility RFS9510 device is upgraded.
	`upgrade [ap621|ap622|br650|br6511|ap6521|br1220|ap6532|ap6562|br71xx|br81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx9000] precedence <1-10000> [cdp-match <LOCATION-SUBSTRING>|dhcp-option <DHCP-OPTION>|fqdn <FQDN>|ip [<START-IP> <END-IP>|<IP/MASK>]|lldp-match <LLDP-STRING>|mac <START-MAC> {<END-MAC>}|model-number <MODEL-NUMBER>|serial-number <SERIAL-NUMBER>|vlan <VLAN-ID>]|lldp-match <LLDP-STRING>|mac <STARTING-MAC> {<ENDING-MAC>}|model-number <MODEL-NUMBER>|serial-number <SERIAL-NUMBER>|vlan <VLAN-ID>]`
redirect	Adds a device upgrade rule. The rule applies to the device type selected. Specify the device type and assign a precedence to the rule. The different device types are: • Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point • Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000 • Service Platforms — Brocade Mobility RFS9510
precedence <1-10000>	Sets the rule precedence. Rules with lower values get precedence over rules with higher values.
cdp-match <LOCATION-SUBSTRING>	Configures the device location to match, based on CDP snoop strings • <LOCATION-SUBSTRING> – Specify the location. Devices matching the specified string are upgraded.
dhcp-option <DHCP-OPTION>	Configures the DHCP options to match DHCP options identify the vendor and DHCP client functionalities. This information is used by the client to convey to the DHCP server that the client requires extra information in a DHCP response. • <DHCP-OPTION> – Specify the DHCP option value. Devices matching the specified value are upgraded.

fqdn <FQDN>	Configures the FQDN to match FQDN is a domain name that specifies its exact location in the DNS hierarchy. It specifies all domain levels, including its top-level domain and the root domain. • <FQDN> – Specify the FQDN. Devices matching the specified value are upgraded.
ip [<START-IP> <END-IP>|<IP/MASK>]	Configures a range of IP addresses and subnet address. Devices having IP addresses within the specified range or are part of the specified subnet are upgraded. • <START-IP> – Specify the first IP address in the range. • <END-IP> – Specify the last IP address in the range. • <IP/MASK> – Specify the IP subnet and mask to match against the device's IP address.
lldp-match <LLDP-STRING>	Configures the device location to match, based on LLDP snoop strings LLDP is a vendor neutral link layer protocol used to advertise a network device's identity, capabilities, and neighbors on a local area network. • <LLDP-STRING> – Specify the location. Devices matching the specified string are upgraded.
mac <START-MAC> {<END-MAC>}	Configures a single or a range of MAC addresses. Devices matching the specified values are upgraded. • <START-MAC> – Specify the first MAC address in the range. Provide only this MAC address to filter a single device. • <END-MAC> – Optional. Specify the last MAC address in the range.
model-number <MODEL-NUMBER>	Configures the device model number • <MODEL-NUMBER> – Specify the model number. Devices matching the specified model number are upgraded.
serial-number <SERIAL-NUMBER>	Configures the device's serial number • <SERIAL-NUMBER> – Specify the serial number. Devices matching the specified serial number are upgraded.
vlan <VLAN-ID>	Configures the VLAN ID • <VLAN-ID> – Specify the VLAN ID. Devices assigned to the specified VLAN are upgraded.

Example

```
rfs4000-229D58(config-auto-provisioning-policy-test)#upgrade ap621 precedence
1 any

rfs4000-229D58(config-auto-provisioning-policy-test)#upgrade rfs4000
precedence 2 ip 192.168.13.1 192.168.13.5

rfs4000-229D58(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
 upgrade ap621 precedence 1 any
 upgrade rfs4000 precedence 2 ip 192.168.13.1 192.168.13.5
rfs4000-229D58(config-auto-provisioning-policy-test)#
```

Related Commands:

no	Removes an upgrade rule

no

auto-provisioning-policy

Removes a deny, permit, or redirect rule from the specified auto provisioning policy

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no [adopt|default-adoption|deny|redirect|upgrade]

no adopt precedence <1-10000>
no deny precedence <1-10000>
no default-adoption
no redirect precedence <1-10000>
no upgrade precedence <1-10000>
```

Parameters

`no adopt precedence <1-10000>`

adopt precedence <1-10000>	Removes the adoption rule identified by the specified precedence • precedence <1-10000> – Specify the rule precedence.

`no deny precedence <1-10000>`

deny precedence <1-10000>	Removes the deny adoption rule identified by the specified precedence • precedence <1-10000> – Specify the rule precedence.

`no default-adoption`

default-adoption	Removes the default adoption rule. When the default adoption rule is absent, devices not matching any of the configured deny or permit criteria are denied adoption

`no redirect precedence <1-10000>`

redirect precedence <1-10000>	Removes the redirect adoption rule identified by the specified precedence • precedence <1-10000> – Specify the rule precedence.

`no upgrade precedence <1-10000>`

upgrade precedence <1-10000>	Removes the device upgrade rule identified by the specified precedence • precedence <1-10000> – Specify the rule precedence.

Example

```
The following example shows the auto-provisioning-policy ‘test’ settings
before the ‘no’ commands are executed:

rfs4000-229D58(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
 default-adoption
 adopt br81xx precedence 1 profile default-br81xx vlan 1
 deny br71xx precedence 2 model-number AP7131N
 deny br71xx precedence 3 ip 192.168.13.23 192.168.13.23
 redirect br81xx precedence 4 controller 192.168.13.10 ip 192.168.13.25
192.168.13.25
 redirect br81xx precedence 5 controller 192.168.13.10 model-number
AP-8132-66040-US
rfs4000-229D58(config-auto-provisioning-policy-test)#
```

```
rfs4000-229D58(config-auto-provisioning-policy-test)#no default-adoption
rfs4000-229D58(config-auto-provisioning-policy-test)#no deny precedence 2
rfs4000-229D58(config-auto-provisioning-policy-test)#no deny precedence 3
rfs4000-229D58(config-auto-provisioning-policy-test)#no deny precedence 5

The following example shows the auto-provisioning-policy 'test' settings after
the 'no' commands are executed:

rfs4000-229D58(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
 adopt br81xx precedence 1 rf-domain TechPubs vlan 1
 redirect br81xx precedence 4 controller 192.168.13.10 ip 192.168.13.25
192.168.13.25
rfs4000-229D58(config-auto-provisioning-policy-test)#

rfs4000-229D58(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
 upgrade ap621 precedence 1 any
 upgrade rfs4000 precedence 2 ip 192.168.13.1 192.168.13.5
rfs4000-229D58(config-auto-provisioning-policy-test)#

rfs4000-229D58(config-auto-provisioning-policy-test)#no upgrade precedence 1

rfs4000-229D58(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
 upgrade rfs4000 precedence 2 ip 192.168.13.1 192.168.13.5
rfs4000-229D58(config-auto-provisioning-policy-test)#
```

Related Commands:

adopt	Configures an adoption rule
default-adoption	Configures the rule for adopting devices when adopt or deny rules are not defined
deny	Configures a deny adoption rule
redirect	Configures a rule redirecting devices seeking adoption to another controller
upgrade	Configures a rule for upgrade of adopted devices

Chapter

ADVANCED-WIPS-POLICY 10

This chapter summarizes the advanced *Wireless Intrusion Protection Systems* (WIPS) policy commands in the CLI command structure.

WIPS policy provides continuous protection against wireless threats and acts as an additional layer of security complementing wireless VPNs and encryption and authentication policies. WIPS uses dedicated sensor devices designed to actively detect and locate unauthorized AP devices. After detection, they use mitigation techniques to block the devices by manual termination or air lockdown.

Unauthorized APs are untrusted access points that accept client associations. They can be deployed for illegal wireless access to a corporate network, implanted with malicious intent by an attacker, or could just be misconfigured access points that do not adhere to corporate policies. An attacker can install a unauthorized AP with the same ESSID as the authorized WLAN, causing a nearby client to associate to it. The unauthorized AP can then steal user credentials from the client, launch a man-in-the middle attack or take control of wireless clients to launch denial-of-service attacks.

A WIPS server can alternatively be deployed (in conjunction with the wireless controller, access point, or service platform) as a dedicated solution within a separate enclosure. A WIPS deployment provides the following enterprise class security management features and functionality:

- *Threat Detection* - Threat detection is central to a wireless security solution. Threat detection must be robust enough to correctly detect threats and swiftly help protect the network.
- *Rogue Detection and Segregation* - A WIPS policy distinguishes itself by identifying and categorizing nearby access points. WIPS identifies threatening versus non-threatening access points by segregating access points attached to the network (unauthorized APs) from those not attached to the network (neighboring access points). The correct classification of potential threats is critical in order for administrators to act promptly against rogues and not invest in a manual search of neighboring access points to isolate the few attached to the network.
- *Locationing* - Administrators can define the location of wireless clients as they move throughout a site. This allows for the removal of potential rogues through the identification and removal of their connected access points.
- *WEP Cloaking* - WEP Cloaking protects organizations using the *Wired Equivalent Privacy* (WEP) security standard to protect networks from common attempts used to crack encryption keys. There are several freeware WEP cracking tools available and 23 known attacks against the original 802.11 encryption standard; even 128-bit WEP keys take only minutes to crack. WEP Cloaking module enables organizations to operate WEP encrypted networks securely and to preserve their existing investment in client devices.

Use the (config) instance to configure advance WIPS policy commands. To navigate to the advanced WIPS policy instance, use the following commands:

```
<DEVICE>(config)#advanced-wips-policy <POLICY-NAME>

rfs7000-37FABE(config-advanced-wips-policy-test)#?
Advanced WIPS policy Mode commands:
  event               Configure event detection
```

```
no                  Negate a command or set its defaults
server-listen-port  Configure local WIPS server listen port number
terminate           Add a device to the list of devices to be terminated
use                 Set setting to use

clrscr              Clears the display screen
commit              Commit all changes made in this session
do                  Run commands from Exec mode
end                 End current mode and change to EXEC mode
exit                End current mode and down to previous mode
help                Description of the interactive help system
revert              Revert changes
service             Service Commands
show                Show running system information
write               Write running configuration to memory or terminal

rfs7000-37FABE(config-advanced-wips-policy-test)#
```

advanced-wips-policy

Table 8 summarizes advanced WIPS policy configuration commands.

TABLE 8 Advanced-WIPS-Policy-Config Commands

Command	Description	Reference
event	Configures event monitoring settings	page 874
no	Negates a command or sets its default	page 880
server-listen-port	Sets a local WIPS server's listening port	page 882
terminate	Adds a device to a list of terminated devices	page 883
use	Defines the settings used with the advanced WIPS policy	page 883
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

event

advanced-wips-policy

Configures anomalous frame detection in a RF network

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
event [accidental-association|all|crackable-wep-iv-used|dos-cts-flood|

dos-deauthentication-detection|dos-disassociation-detection|dos-eap-failure-s
poof|
          dos-eapol-logoff-storm|dos-rts-flood|essid-jack-attack-detected|

fake-dhcp-server-detected|fata-jack-detected|id-theft-eapol-success-spoof-det
ected|

id-theft-out-of-sequence|invalid-channel-advertized|invalid-management-frame|

ipx-detection|monkey-jack-attack-detected|multicast-all-routers-on-subnet|
          multicast-all-systems-on-subnet|multicast-dhcp-server-relay-agent|

multicast-hsrp-agent|multicast-igmp-detection|multicast-igrp-routers-detectio
n|

multicast-ospf-all-routers-detection|multicast-ospf-designated-routers-detect
ion|

multicast-rip2-routers-detection|multicast-vrrp-agent|netbios-detection|

null-probe-response-detected|probe-response-flood|rogue-br-detection|
          stp-detection|unauthorized-bridge|windows-zero-config-memory-leak|
          wlan-jack-attack-detected]

event accidental-association mitigation-enable
event accidental-association trigger-against
[neighboring|sanctioned|unsanctioned]
          {(neighboring|sanctioned|unsanctioned)}

event all trigger-all-applicable

event [crackable-wep-iv-used|dos-deauthentication-detection|
          dos-disassociation-detection|dos-eap-failure-spoof|dos-rts-flood|

essid-jack-attack-detected|fake-dhcp-server-detected|fata-jack-detected|
          id-theft-eapol-success-spoof-detected|id-theft-out-of-sequence|
          invalid-channel-advertized|invalid-management-frame|ipx-detection|
          monkey-jack-attack-detected|multicast-all-routers-on-subnet|
          multicast-all-systems-on-subnet|multicast-dhcp-server-relay-agent|

multicast-hsrp-agent|multicast-igmp-detection|multicast-igrp-routers-detectio
n|

multicast-ospf-all-routers-detection|multicast-ospf-designated-routers-detect
ion|

multicast-rip2-routers-detection|multicast-vrrp-agent|netbios-detection|
```

```
          null-probe-response-detected|stp-detection|unauthorized-bridge|
          windows-zero-config-memory-leak|wlan-jack-attack-detected]
trigger-against
          [neighboring|sanctioned|unsanctioned]
{(neighboring|sanctioned|unsanctioned)}


event dos-cts-flood threshold [cts-frames-ratio <0-65535>|mu-rx-cts-frame
<0-65535>]
event dos-cts-flood trigger-against [neighboring|sanctioned|unsanctioned]
{(neighboring|sanctioned|unsanctioned)}

event dos-eapol-logoff-storm threshold [eapol-start-frames-br <0-65535>|
          eapol-start-frames-mu <0-65535>]
event dos-eapol-logoff-storm trigger-against
[neighboring|sanctioned|unsanctioned]
          {(neighboring|sanctioned|unsanctioned)}

event probe-response-flood threshold probe-rsp-frames-count <0-65535>
event probe-response-flood trigger-against
[neighboring|sanctioned|unsanctioned]
          {(neighboring|sanctioned|unsanctioned)}

event rogue-br-detection mitigation-enable
event rogue-br-detection trigger-against
[neighboring|sanctioned|unsanctioned]
          {(neighboring|sanctioned|unsanctioned)}
```

Parameters

```
event accidental-association mitigation-enable
```

accidental-association	This event occurs when an authorized station/client connects accidentally to an unauthorized or ignored access point/controller.
mitigation-enable	Enables the default mitigation of an accidental association event

```
event accidental-association trigger-against
[neighboring|sanctioned|unsanctioned]
{(neighboring|sanctioned|unsanctioned)}
```

accidental-association	This event occurs when an authorized station/client connects accidentally to an unauthorized or ignored access point/wireless controller.
trigger-against [neighboring| sanctioned| unsanctioned]	The accidental association event is triggered when one or all of the following events occur: • neighboring – When neighboring client devices associate • sanctioned – When sanctioned devices associate • unsanctioned – When unsanctioned devices associate

```
event all trigger-all-applicable
```

all trigger-all-applicable	Enables triggers for all events

```
event
[crackable-wep-iv-used|dos-deauthentication-detection|dos-disassociation-
detection|dos-eap-failure-spoof|dos-rts-flood|essid-jack-attack-detected|
fake-dhcp-server-detected|fata-jack-detected|id-theft-eapol-success-spoof-det
ected|
id-theft-out-of-sequence|invalid-channel-advertized|invalid-management-frame|
ipx-detection|monkey-jack-attack-detected|multicast-all-routers-on-subnet|
multicast-all-systems-on-subnet|multicast-dhcp-server-relay-agent|
```

	`multicast-hsrp-agent|multicast-igmp-detection|multicast-igrp-routers-detection|`
	`multicast-ospf-all-routers-detection|multicast-ospf-designated-routers-detection|`
	`multicast-rip2-routers-detection|multicast-vrrp-agent|netbios-detection|`
	`null-probe-response-detected|stp-detection|unauthorized-bridge|`
	`windows-zero-config-memory-leak|wlan-jack-attack-detected] trigger-against [neighboring|sanctioned|unsanctioned]` *`{(neighboring|sanctioned|unsanctioned)}`*

crackable-wep-iv-used	This event occurs when a crackable WEP initialization vector is used. The standard WEP64 uses a 40 bit key concatenated with a 24 bit initialization vector
dos-deauthentication-detection	This event occurs when a DoS deauthentication attack is detected. In this attack, clients connected to an AP are constantly forced to deauthenticate so they cannot stay connected to the network long enough to utilize it.
dos-disassociation-detection	This event occurs when a DoS disassociation attack is detected. With this attack, clients connected to an AP are constantly disassociated. A fake disassociation frame is generated using an AP MAC address as the source address and the MAC address of the target device as the destination address. The target device on receiving this fake frame dissociates itself from the AP, then tries to re-associate. If the target receives a large number of disassociation frames, it will not be able to stay connected to the network long enough to utilize it.
dos-eap-failure-spoof	This event occurs when a DoS EAP failure spoofing attack is detected. The attacker generates a large number of EAP-failure packets forcing the AP to disassociate with its legitimate wireless clients.
dos-rts-flood	This event occurs when a large number of *request to send* (RTS) frames are detected in the network.
essid-jack-attack-detected	This event occurs when an essid-jack attack is detected. Essid-jack is a tool in the AirJack suite that sends a disassociate frame to a target client to force it to reassociate it to the network to find the SSID. This can be used to launch further DoS attacks on the network.
fake-dhcp-server-detected	This event occurs when a fake DHCP server is detected. A fake or rogue DHCP server is a type of man in the middle attack where DHCP services are provide by an unauthorized DHCP server compromising the integrity of the controller managed network.
fata-jack-detected	This event occurs when a FATA-jack exploit is detected. FATA-jack is a tool in the AirJack suite that forces an AP to disassociate a valid client. This exploit uses a spoofed authentication frame with an invalid authentication algorithm number of 2. The attacker sends an invalid authentication frame with the wireless client's MAC, forcing the AP to return a deauth to the client.
id-theft-eapol-success-spoof-detected	This event occurs when an EAPOL success spoof is detected The attacker keeps the client from providing its credentials through the EAP-response packet by sending a EAP-success packet. Since the client is unable to provide its credentials, it cannot be authenticated and therefore cannot access the wireless network.
id-theft-out-of-sequence	This event occurs when an out of sequence packet is received. This indicates a wireless client has been spoofed and is sending a packet out of sequence with the packet sent by the real wireless client (that means two devices using the same MAC address have been detected operating in the airspace, resulting in detected wireless frames that are out of sequence)
invalid-channel-advertized	This event occurs when packets with invalid channels are detected.
invalid-management-frame	This event occurs when an invalid management frame is detected.
ipx-detection	This event occurs when Novell's *Internetwork Packet Exchange* (IPX) packets are detected
monkey-jack-attack-detected	This event occurs when a monkey-jack attack is detected. Monkey-jack is a tool in the AirJack suite that enables an attacker to deauthenticate all wireless clients from an AP, and then insert itself between the AP and the wireless clients.
multicast-all-routers-on-subnet	This event occurs when a sanctioned device detects multicast packets to all routers on the subnet

multicast-all-systems-on-subnet	This event occurs when a sanctioned device detects multicast packets to all systems on the subnet
multicast-dhcp-server-relay-agent	This event occurs when a sanctioned device detects a DHCP server relay agent in the network
multicast-hsrp-agent	This event occurs when a sanctioned device detects a *Hot Standby Router Protocol* (HSRP) agent in the network
multicast-igmp-detection	This event occurs when a sanctioned device detects multicast *Internet Group Management Protocol* (IGMP) packets.
multicast-igrp-routers-detection	This event occurs when a sanctioned device detects multicast *Interior Gateway Routing Protocol* (IGRP) packets.
multicast-ospf-all-routers-detection	This event occurs when a sanctioned device detects multicast *Open Shortest Path First* (OSPF).packets
multicast-ospf-designated-routers-detection	This event occurs when a sanctioned device detects multicast OSPF routers in the network.
multicast-rip2-routers-detection	This event occurs when a sanctioned device detects multicast *Routing Information Protocol version 2* (RIP2) routers in the network.
multicast-vrrp-agent	This event occurs when a sanctioned device detects multicast *Virtual Router Redundancy Protocol* (VRRP) agents in the network.
netbios-detection	This event occurs when netbios packets are detected in the network. *Network Basic Input/Output System* (netbios) provides services related to the sessions layer of the OSI model. This allows applications on different devices to communicate over the local area network.
null-probe-response-detected	This event occurs when a sanctioned device detects null probe response packets.
stp-detection	This event occurs when a sanctioned device detects *Scanning Tunnelling Protocol* (STP) packets in the network.
unauthorized-bridge	This event occurs when unauthorized bridges are detected in the network.
windows-zero-config-memory-leak	This event occurs when a Windows™ Zero-Config memory leak is detected.
wlan-jack-attack-detected	This event occurs when a WLAN-jack exploit is detected. WLAN-jack is a tool in the AirJack suite that forces an AP to disassociate a valid client. The attacker sends deauthentication frames continuously or uses the broadcast address. This prevents the wireless clients from reassociating with the AP.

trigger-against [neighboring| sanctioned| unsanctioned]	The following keywords are common to all of the above events:
	• trigger-against – Configures the event trigger condition
	  • neighboring – The selected event is triggered only against neighboring devices
	  • sanctioned – The selected event is triggered only against sanctioned devices
	  • unsanctioned – The selected event is triggered only against unsanctioned devices

	`event dos-cts-flood threshold [cts-frames-ratio <0-65535>|mu-rx-cts-frame <0-65535>]`
dos-cts-flood	This event occurs when a large number of *clear to send* (CTS) frames are detected in the network

threshold [cts-frames-ratio <0-65535>| mu-rx-cts-frame <0-65535>]	Sets the CTS flood threshold
	• cts-frames-radio <0-65535> – Sets the CTS:Total Frames ratio for triggering this event
	  • <0-65535> – Specify the value from 0 - 65535.
	• mu-rx-cts-frame – Sets the CTS frame received by clients
	  • <0-65535> – Specify the value from 0 - 65535.

	`event dos-cts-flood trigger-against [neighboring|sanctioned|unsanctioned] {(neighboring|sanctioned|unsanctioned)}`
dos-cts-flood	This event occurs when a large number of CTS frames are detected in the network
trigger-against (neighboring, sanctioned, unsanctioned)	Sets the event trigger condition • sanctioned – An event is triggered only against sanctioned devices • unsanctioned – An event is triggered only against unsanctioned devices • neighboring – An event is triggered only against neighboring devices

	`event dos-eapol-logoff-storm threshold [eapol-start-frames-br <0-65535>| eapol-start-frames-mu <0-65535>]`
dos-eapol-logoff-storm	This event occurs when a large number of EAPOL logoff frames are detected in the network
threshold [eapol-start-frames-br <0-65535>| eapol-start-frames-mu <0-65535>]	Sets the EAPOL logoff frames flood threshold • eapol-start-frames-br – Sets the EAPOL start frames transmitted by an AP to trigger this event • <0-65535> – Specify a value from 0 - 65535. • eapol-start-frames-mu – Sets the EAPOL start frames transmitted by a client to trigger this event • <0-65535> – Specify a value from 0 - 65535.

	`event dos-eapol-logoff-storm trigger-against [neighboring|sanctioned|unsanctioned] {(neighboring|sanctioned|unsanctioned)}`
dos-eapol-logoff-storm	This event occurs when a large number of EAPOL logoff frames are detected in the network
trigger-against (neighboring, sanctioned, unsanctioned)	Sets the event trigger condition • sanctioned – An event is triggered only against sanctioned devices • unsanctioned – An event is triggered only against unsanctioned devices • neighboring – An event is triggered only against neighboring devices

	`event probe-response-flood threshold probe-rsp-frames-count <0-65535>`
probe-response-flood	This event occurs when a large number of probe response frames are detected in the network
threshold probe-rsp-frames-count <0-65535>	Sets the probe response frames flood threshold • probe-rsp-frames-count – Sets the threshold from the number of probe response frames received • <0-65535> – Specify the value from 0 - 65535.

	`event probe-response-flood trigger-against [neighboring|sanctioned|unsanctioned] {(neighboring|sanctioned|unsanctioned)}`
probe-response-flood	This event occurs when a large number of probe response frames are detected in the network
trigger-against (neighboring, sanctioned, unsanctioned)	Sets the event trigger condition • sanctioned – An event is triggered only against sanctioned devices • unsanctioned – An event is triggered only against unsanctioned devices • neighboring – An event is triggered only against neighboring devices

	`event rogue-br-detection mitigation-enable`
rogue-br-detection	This event occurs when rogue APs are detected in the network
mitigation-enable	Enables default mitigation for the rogue-br-detection event

```
event rogue-br-detection trigger-against
[neighboring|sanctioned|unsanctioned] {(neighboring|sanctioned|unsanctioned)}
```

rogue-br-detection	This event occurs when rogue APs are detected in the network.
trigger-against (neighboring, sanctioned, unsanctioned)	Sets the trigger condition • sanctioned – An accidental association event is triggered against sanctioned devices • unsanctioned – An accidental association event is triggered against unsanctioned devices • neighboring – An accidental association event is triggered against neighboring devices

Example

```
rfs7000-37FABE(config-advanced-wips-policy-test)#event dos-cts-flood
threshold cts-frames-ratio 8
rfs7000-37FABE(config-advanced-wips-policy-test)#event dos-eapol-logoff-storm
threshold eapol-start-frames-mu 99
rfs7000-37FABE(config-advanced-wips-policy-test)#event probe-response-flood
threshold probe-rsp-frames-count 8
rfs7000-37FABE(config-advanced-wips-policy-test)#event
wlan-jack-attack-detected trigger-against sanctioned
rfs7000-37FABE(config-advanced-wips-policy-test)#event probe-response-flood
trigger-against sanctioned

rfs7000-37FABE(config-advanced-wips-policy-test)#show context
advanced-wips-policy test
 event wlan-jack-attack-detected trigger-against sanctioned
 event probe-response-flood trigger-against sanctioned
 event probe-response-flood threshold probe-rsp-frames-count 8
 no event dos-cts-flood trigger-against
 event dos-cts-flood threshold cts-frames-ratio 8
 no event dos-eapol-logoff-storm trigger-against
 event dos-eapol-logoff-storm threshold eapol-start-frames-mu 99
rfs7000-37FABE(config-advanced-wips-policy-test)#
```

Related Commands:

no	Removes or resets triggers against various events

no

advanced-wips-policy

Negates a command or reverts settings to their default

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no [event|server-listen-port|terminate|use]

no event <EVENT-NAME>
```

```
no server-listen-port

no terminate <MAC>

no use device-configuration
```

Parameters

```
no event <EVENT-NAME>
```

no event <EVENT-NAME>	Disables event handling for the event specified as its parameter See *event* for more information on each of the parameters.

```
no server-listen-port
```

no server-listen-port	Resets the listen port for WIPS sensors to its default

```
no terminate <MAC>
```

terminate <MAC>	Removes a device, identified by its MAC address, from the device termination list

```
no use device-configuration
```

no use device-categorization	Removes the current device categorization list from the advanced WIPS policy

Example

```
The following example shows the WIPS policy ‘test’ settings before the ‘no’
commands are executed:

rfs7000-37FABE(config-advanced-wips-policy-test)#show context
advanced-wips-policy test
 event wlan-jack-attack-detected trigger-against sanctioned
 event probe-response-flood trigger-against sanctioned
 event probe-response-flood threshold probe-rsp-frames-count 8
 no event dos-cts-flood trigger-against
 event dos-cts-flood threshold cts-frames-ratio 8
 no event dos-eapol-logoff-storm trigger-against
 event dos-eapol-logoff-storm threshold eapol-start-frames-mu 99
rfs7000-37FABE(config-advanced-wips-policy-test)#

rfs7000-37FABE(config-advanced-wips-policy-test)#no event
wlan-jack-attack-detected trigger-against
rfs7000-37FABE(config-advanced-wips-policy-test)#no event
probe-response-flood trigger-against
rfs7000-37FABE(config-advanced-wips-policy-test)#no event
probe-response-flood threshold probe-rsp-frames-count
rfs7000-37FABE(config-advanced-wips-policy-test)#no event
dos-eapol-logoff-storm
 trigger-against

The following example shows the WIPS policy ‘test ‘settings after the ‘no’
commands are executed:

rfs7000-37FABE(config-advanced-wips-policy-test)#show context
advanced-wips-policy test
 no event dos-cts-flood trigger-against
 event dos-cts-flood threshold cts-frames-ratio 8
 no event dos-eapol-logoff-storm trigger-against
```

```
 event dos-eapol-logoff-storm threshold eapol-start-frames-mu 99
rfs7000-37FABE(config-advanced-wips-policy-test)#
```

Related Commands:

event	Configures WIPS events
server-listen-port	Defines the port where WIPS sensors connect to the WIPS server
terminate	Adds a device to the device terminate list
use	Configures the device categorization list used with the advanced WIPS policy

server-listen-port

advanced-wips-policy

Defines the local advanced WIPS server's listening port, where WIPS sensors connect to the local WIPS server

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
server-listen-port <0-65535>
```

Parameters

```
server-listen-port <0-65535>
```

server-listen-port <0-65535>	Select a port from 0 - 65535.

NOTE
Onboard WIPS uses port 8443 and AirDefense Enterprise uses 443.

Example

```
rfs7000-37FABE(config-advanced-wips-policy-test)#server-listen-port 1009

rfs7000-37FABE(config-advanced-wips-policy-test)#show context
advanced-wips-policy test
 server-listen-port 1009
 no event dos-cts-flood trigger-against
 event dos-cts-flood threshold cts-frames-ratio 8
 no event dos-eapol-logoff-storm trigger-against
 event dos-eapol-logoff-storm threshold eapol-start-frames-mu 99
rfs7000-37FABE(config-advanced-wips-policy-test)#
```

Related Commands:

no	Resets local WIPS server's listening port to default

terminate

advanced-wips-policy

Adds a device to a device termination list. Devices on this list cannot access the network.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
terminate <MAC>
```

Parameters

```
terminate <MAC>
```

terminate <MAC>	Adds a device's MAC address to the device termination list. Devices on this list cannot access the network. • <MAC> – Specify the device's MAC address. Device's added to the termination list (identified by their MAC addresses) are removed from connection within the managed network. Therefore, be sure they represent potential threats.

Example

```
rfs7000-37FABE(config-advanced-wips-policy-test)#terminate 00-40-96-B0-BA-2D

rfs7000-37FABE(config-advanced-wips-policy-test)#show context
advanced-wips-policy test
 terminate 00-40-96-B0-BA-2D
 server-listen-port 1009
 no event dos-cts-flood trigger-against
 event dos-cts-flood threshold cts-frames-ratio 8
 no event dos-eapol-logoff-storm trigger-against
 event dos-eapol-logoff-storm threshold eapol-start-frames-mu 99
rfs7000-37FABE(config-advanced-wips-policy-test)#
```

Related Commands:

no	Removes a device from the device termination list

use

advanced-wips-policy

Uses an existing device categorization list with the advanced WIPS policy. A device configuration list must exist before it can be used with the advanced WIPS policy.

A device categorization list categorizes a device, either an AP or a wireless client, as sanctioned or neighboring based on its MAC address or access point SSID.

For more information on creating a device categorization list, see *device-categorization*.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
use device-categorization <DEVICE-CATEGORIZATION-LIST>
```

Parameters

```
use device-categorization <DEVICE-CATEGORIZATION-LIST>
```

device-categorization <DEVICE-CATEGORIZATION-LIST>	Associates a device categorization list with the profile • <DEVICE-CATEGORIZATION-LIST> – Specify a device categorization list name.

NOTE
Advanced WIPS ignores the SSID of marked devices for device categorization.

Example

```
rfs7000-37FABE(config-advanced-wips-policy-test)#use device-categorization
test
Please note, advanced-wips ignores SSID of marked devices
rfs7000-37FABE(config-advanced-wips-policy-test)#

rfs7000-37FABE(config-advanced-wips-policy-test)#show context
advanced-wips-policy test
 terminate 00-40-96-B0-BA-2D
 use device-categorization test
 server-listen-port 1009
 no event dos-cts-flood trigger-against
 event dos-cts-flood threshold cts-frames-ratio 8
 no event dos-eapol-logoff-storm trigger-against
 event dos-eapol-logoff-storm threshold eapol-start-frames-mu 99
rfs7000-37FABE(config-advanced-wips-policy-test)#
```

Related Commands:

no	Resets values or disables commands
device-categorization	Creates a device categorization list

Chapter

ASSOCIATION-ACL-POLICY 11

This chapter summarizes the association ACL policy commands in the CLI command structure. An association ACL is a
policy-based *Access Control List* (ACL) that either prevents or allows wireless clients from connecting to a controller managed WLAN.

System administrators can use an association ACL to grant or restrict wireless clients access to the WLAN by specifying client MAC addresses or range of MAC addresses to either include or exclude from controller connectivity. Association ACLs are applied to WLANs as an additional access control mechanism.

Use the (config) instance to configure the association ACL policy. To navigate to the association-acl-policy instance, use the following commands:

```
<DEVICE>(config)#association-acl-policy <POLICY-NAME>

rfs7000-37FABE(config)#association-acl-policy test
rfs7000-37FABE(config-assoc-acl-test)#

rfs7000-37FABE(config-assoc-acl-test)#?
Association ACL Mode commands:
  deny     Specify MAC addresses to be denied
  no       Negate a command or set its defaults
  permit   Specify MAC addresses to be permitted

  clrscr   Clears the display screen
  commit   Commit all changes made in this session
  do       Run commands from Exec mode
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  revert   Revert changes
  service  Service Commands
  show     Show running system information
  write    Write running configuration to memory or terminal

rfs7000-37FABE(config-assoc-acl-test)#
```

NOTE
If creating an new association ACL policy, provide a name specific to its function. Avoid naming it after a WLAN it may support. The name cannot exceed 32 characters.

Before defining an association ACL policy and applying it to a WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- The name and configuration of an association ACL policy should meet the requirements of the WLANs it may map to. However, be careful not to name ACLs after specific WLANs, as individual ACL policies can be used by more than one WLAN.
- You cannot apply more than one MAC based ACL to a layer 2 interface. If a MAC ACL is already configured on a layer 2 interface, and a new MAC ACL is applied to the interface, the new ACL replaces the previously configured one.

association-acl-policy

ASSOCIATION-ACL-POLICY

Table 9 summarizes association ACL policy configuration commands.

TABLE 9 Association-ACL-Policy-Config Commands

Command	Description	Reference
deny	Specifies a range of MAC addresses denied access to the WLAN	page 886
no	Removes a deny or permit rule from this association ACL policy	page 887
permit	Specifies a range of MAC addresses allowed access to the WLAN	page 889
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

deny

association-acl-policy

Creates a list of devices denied access to the managed network. Devices are identified by their MAC address. A single MAC address or a range of MAC addresses can be denied access. This command also sets the precedence on how deny rules are applied. Up to a thousand (1000) deny rules can be defined for every association ACL policy. Each rule has a unique sequential precedence value assigned, and are applied to packets on the basis of this precedence value. Lower the precedence of a rule, higher is its priority. This results in the rule with the lowest precedence being applied first. No two rules can have the same precedence. The default precedence is 1, so be careful to prioritize ACLs accordingly as they are added.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
deny <STARTING-MAC> [<ENDING-MAC>|precedence]

deny <STARTING-MAC> precedence <1-1000>
```

```
deny <STARTING-MAC> <ENDING-MAC> precedence <1-1000>
```

Parameters

```
deny <STARTING-MAC> precedence <1-1000>
```

deny	Adds a single device or a set of devices to the deny list
<STARTING-MAC>	To add a single device, enter its MAC address in the <STARTING-MAC> parameter.
precedence <1-1000>	Sets a precedence rule. Rules are applied in an increasing order of precedence. • <1-1000> – Specify a precedence value from 1 - 1000.

```
deny <STARTING-MAC> <ENDING-MAC> precedence <1-1000>
```

deny	Adds a single device or a set of devices to the deny list To add a set of devices, provide the range of MAC addresses.
<STARTING-MAC>	Specify the first MAC address in the range.
<ENDING-MAC>	Specify the last MAC address in the range.
precedence <1-1000>	Sets a precedence rule. Rules are applied in an increasing order of precedence. • <1-1000> – Specify a value from 1 - 1000.

Usage Guidelines:

Every rule has a unique sequential precedence value. You cannot add two rules with the same precedence. Rules are applied in an increasing order of precedence. That means the rule with precedence 1 is applied first, then the rule with precedence 2 and so on.

Example

```
rfs7000-37FABE(config-assoc-acl-test)#deny 11-22-33-44-55-01
11-22-33-44-55-FF precedence 150

rfs7000-37FABE(config-assoc-acl-test)#deny 11-22-33-44-56-01
11-22-33-44-56-01 precedence 160

rfs7000-37FABE(config-assoc-acl-test)#show context
association-acl-policy test
 deny 11-22-33-44-55-01 11-22-33-44-55-FF precedence 150
 deny 11-22-33-44-56-01 11-22-33-44-56-01 precedence 160
rfs7000-37FABE(config-assoc-acl-test)#
```

Related Commands:

no	Removes a deny rule based on its precedence value

no

association-acl-policy

Removes a deny or permit rule from this association ACL policy

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no [deny|permit]

no deny <STARTING-MAC> precedence <1-1000>
no deny <STARTING-MAC> <ENDING-MAC> precedence <1-1000>

no permit <STARTING-MAC> precedence <1-1000>
no permit <STARTING-MAC> <ENDING-MAC> precedence <1-1000>
```

Parameters

`deny <STARTING-MAC> precedence <1-1000>`

no deny	Removes a single device or a set of devices from the deny list
<STARTING-MAC>	To remove a single device, enter its MAC address in the <STARTING-MAC> parameter.
precedence <1-1000>	Specifies the rule precedence • <1-1000> – Specify the value from 1 - 1000.

`deny <STARTING-MAC> <ENDING-MAC> precedence <1-1000>`

no deny	Removes a single device or a set of devices from the deny list To remove a set of devices, enter the MAC address range.
<STARTING-MAC>	Specify the first MAC address in the range.
<ENDING-MAC>	Specify the last MAC address in the range.
precedence <1-1000>	Specifies the rule precedence • <1-1000> – Specify a value from 1 - 1000.

`no permit <STARTING-MAC> precedence <1-1000>`

no permit	Removes a single device or a set of devices from the permit list
<STARTING-MAC>	To remove a single device, enter its MAC address in the <STARTING-MAC> parameter.
precedence <1-1000>	Specifies the rule precedence • <1-1000> – Specify a value from 1 - 1000.

`no permit <STARTING-MAC> <ENDING-MAC> precedence <1-1000>`

no permit	Removes a single device or a set of devices from the permit list To remove a set of devices, enter the MAC address range.
<STARTING-MAC>	Specify the first MAC address in the range.
<ENDING-MAC>	Specify the last MAC address in the range.
precedence <1-1000>	Specifies the rule precedence • <1-1000> – Specify a value from 1 - 1000.

Example

```
The following example shows the association ACL policy ‘test’ settings before
the ‘no’ commands is executed:

rfs7000-37FABE(config-assoc-acl-test)#show context
association-acl-policy test
```

```
 deny 11-22-33-44-55-01 11-22-33-44-55-FF precedence 150
 deny 11-22-33-44-56-01 11-22-33-44-56-01 precedence 160
rfs7000-37FABE(config-assoc-acl-test)#

rfs7000-37FABE(config-assoc-acl-test)#no deny 11-22-33-44-56-01
11-22-33-44-56-FF precedence 160

The following example shows the association ACL policy ‘test’ settings after
the ‘no’ commands is executed:

rfs7000-37FABE(config-assoc-acl-test)#show context
association-acl-policy test
 deny 11-22-33-44-55-01 11-22-33-44-55-FF precedence 150
rfs7000-37FABE(config-assoc-acl-test)#
```

Related Commands:

deny	Adds a device or a set of devices to the deny list
permit	Adds a device or a set of devices to the permit list

permit

association-acl-policy

Creates a list of devices allowed access to the managed network. Devices are permitted access based on their MAC address. A single MAC address or a range of MAC addresses can be specified. This command also sets the precedence on how permit list rules are applied. Up to a thousand (1000) permit rules can be defined for every association ACL policy. Each rule has a unique sequential precedence value assigned, and are applied to packets on the basis of this precedence value. Lower the precedence of a rule, higher is its priority. This results in the rule with the lowest precedence being applied first. No two rules can have the same precedence. The default precedence is 1, so be careful to prioritize ACLs accordingly as they are added.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
permit <STARTING-MAC> [<ENDING-MAC>|precedence]

permit <STARTING-MAC> precedence <1-1000>
permit <STARTING-MAC> <ENDING-MAC> precedence <1-1000>
```

Parameters

```
permit <STARTING-MAC> precedence <1-1000>
```

permit	Adds a single device or a set of devices to the permit list

<STARTING-MAC>	To add a single device, enter its MAC address in the <STARTING-MAC> parameter.
precedence <1-1000>	Specifies a rule precedence. Rules are applied in an increasing order of precedence. • <1-1000> – Specify a value from 1 - 1000.

```
permit <STARTING-MAC> <ENDING-MAC> precedence <1-1000>
```

permit	Adds a single device or a set of devices to the permit list To add a set of devices, provide the MAC address range.
<STARTING-MAC>	Specify the first MAC address of the range.
<ENDING-MAC>	Specify the last MAC address of the range.
precedence <1-1000>	Specifies a rule precedence. Rules are applied in an increasing order of precedence. • <1-1000> – Specify a value from 1 - 1000.

Usage Guidelines:

Every rule has a unique sequential precedence value. You cannot add two rules with the same precedence. Rules are applied to packets in an increasing order of precedence. That means the rule with precedence 1 is applied first, then the rule with precedence 2 and so on.

Example

```
rfs7000-37FABE(config-assoc-acl-test)# permit 11-22-33-44-66-01
11-22-33-44-66-FF precedence 170

rfs7000-37FABE(config-assoc-acl-test)# permit 11-22-33-44-67-01 precedence 180

rfs7000-37FABE(config-assoc-acl-test)#show context
association-acl-policy test
 deny 11-22-33-44-55-01 11-22-33-44-55-FF precedence 150
 permit 11-22-33-44-66-01 11-22-33-44-66-FF precedence 170
 permit 11-22-33-44-67-01 11-22-33-44-67-01 precedence 180
rfs7000-37FABE(config-assoc-acl-test)#
```

Related Commands:

no	Removes a permit rule based on its precedence

Chapter

ACCESS-LIST 12

This chapter summarizes IP and MAC access list commands in the CLI command structure.

Access lists control access to the managed network using a set of rules also known as *Access Control Entries* (ACEs). Each rule specifies an action taken when a packet matches that rule. If the action is deny, the packet is dropped. If the action is permit, the packet is allowed. A set of deny and/or permit rules based on IP addresses constitutes a IP *Access Control List* (ACL). Similarly, a set of deny and/or permit rules based on MAC addresses constitutes a MAC ACL.

Within a managed network, IP ACLs are used as firewalls to filter packets, and may also mark packets, based on the IP address from which they arrive, as opposed to filtering packets on layer 2 ports. IP based firewall rules are specific to the source and destination IP addresses and have unique precedence orders assigned. Both IP and non-IP traffic on the same layer 2 or port interface can be filtered by applying an IP ACL.

MAC ACLs are firewalls that filter or mark packets based on the MAC address from which they arrive, as opposed to filtering packets on layer 2 ports. Optionally filter layer 2 traffic on a physical layer 2 interface using MAC addresses. A MAC firewall rule uses source and destination MAC addresses for matching operations, where the result is a typical allow, deny or mark designation to controller managed packet traffic.

The following ACLs are supported:

- *ip-access-list*
- *mac-access-list*

Use IP and MAC commands under the global configuration to create an access list.

- When the access list is applied on an Ethernet port, it becomes a port ACL
- When the access list is applied on a VLAN interface, it becomes a router ACL

Use the (config) instance to configure a new ACL or modify an existing ACL. To navigate to the (config-access-list) instance, use the following commands:

```
<DEVICE>(config)#ip access-list <IP-ACCESS-LIST-NAME>

<DEVICE>(config)#mac access-list <MAC-ACCESS-LIST-NAME>
```

NOTE
If creating an new ACL policy, provide a name that uniquely identifies its purpose. The name cannot exceed 32 characters.

ip-access-list

```
rfs7000-37FABE(config)#ip access-list test
rfs7000-37FABE(config-ip-acl-test)#?
ACL Configuration commands:
  deny     Specify packets to reject
  disable  Disable rule if not needed
  insert   Insert this rule (instead of overwriting a existing rule)
  no       Negate a command or set its defaults
  permit   Specify packets to forward
```

```
  clrscr   Clears the display screen
  commit   Commit all changes made in this session
  do       Run commands from Exec mode
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  revert   Revert changes
  service  Service Commands
  show     Show running system information
  write    Write running configuration to memory or terminal

rfs7000-37FABE(config-ip-acl-test)#
```

mac-access-list

```
rfs7000-37FABE(config)#mac access-list test
rfs7000-37FABE(config-mac-acl-test)#?
MAC Extended ACL Configuration commands:
  deny     Specify packets to reject
  disable  Disable rule if not needed
  insert   Insert this rule (instead of overwriting a existing rule)
  no       Negate a command or set its defaults
  permit   Specify packets to forward

  clrscr   Clears the display screen
  do       Run commands from Exec mode
  commit   Commit all changes made in this session
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  revert   Revert changes
  service  Service Commands
  show     Show running system information
  write    Write running configuration to memory or terminal

rfs7000-37FABE(config-mac-acl-test)#
```

ip-access-list

ACCESS-LIST

Table 10 summarizes IP access list configuration commands.

TABLE 10 IP-Access-List-Config Commands

Command	Description	Reference
deny	Creates a deny access rule or modifies an existing rule. A deny access rule rejects packets from specified address(es) and/or destined for specified address(es).	page 893
disable	Disables an existing deny or permit rule without removing it from the ACL	page 902
insert	Inserts a rule in an IP ACL without overwriting or replacing an existing rule having the same precedence	page 904
no	Removes a deny and/or a permit access rule from a IP ACL	page 906
permit	Creates a permit access rule or modifies an existing rule. A permit access rule accepts packets from specified address(es) and/or destined for specified address(es).	page 908

TABLE 10 IP-Access-List-Config Commands

Command	Description	Reference
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

deny

ip-access-list

Creates a deny rule that rejects packets from a specified source IP and/or to a specified destination IP. You can also use this command to modify an existing deny rule.

NOTE
Use a decimal value representation to implement a `permit/deny` designation for a packet. The command set for IP ACLs provides the hexadecimal values for each listed EtherType. Use the decimal equivalent of the EtherType listed for any other EtherType.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
deny [<NETWORK-SERVICE-ALIAS-NAME>|icmp|ip|proto|tcp|udp]

deny <NETWORK-SERVICE-ALIAS-NAME>
[<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|
          from-vlan <VLAN-ID>|host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|any|host
<DEST-HOST-IP>|
          <NETWORK-GROUP-ALIAS-NAME>] (log,mark [8021p <0-7>|dscp <0-63>],
          rule-precedence <1-5000>) {(rule-description <LINE>)}
```

```
deny icmp [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan
<VLAN-ID>|
          host <SOURCE-HOST-IP>]
[<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|
          host <DEST-HOST-IP>] (<ICMP-TYPE> <ICMP-CODE>,log,rule-precedence
<1-5000>)
          {(rule-description <LINE>)}

deny ip [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>|
          host <SOURCE-HOST-IP>]
[<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|
          host <DEST-HOST-IP>] (log,rule-precedence <1-5000>) {(
rule-description <LINE>)}

deny proto [<PROTOCOL-NUMBER>|<PROTOCOL-NAME>|eigrp|gre|igmp|igp|ospf|vrrp]
          [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan
<VLAN-ID>|
          host <SOURCE-HOST-IP>]
[<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|
          host <DEST-HOST-IP>] (log,rule-precedence <1-5000>)
{(rule-description <LINE>)}

deny [tcp|udp] [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan
<VLAN-ID>|
          host <SOURCE-HOST-IP>]
[<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|
          eq <SOURCE-PORT>|host <DEST-HOST-IP>|range <START-PORT> <END-PORT>]
          [eq
[<1-65535>|<SERVICE-NAME>|bgp|dns|ftp|ftp-data|gopher|https|ldap|nntp|ntp|pop
3|
          sip|smtp|ssh|telnet|tftp|www]|range <START-PORT> <END-PORT>]
          (log,rule-precedence <1-5000>) {(rule-description <LINE>)}
```

Parameters

```
deny <NETWORK-SERVICE-ALIAS-NAME>
[<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|
from-vlan <VLAN-ID>|host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|any|host
<DEST-HOST-IP>|
<NETWORK-GROUP-ALIAS-NAME>] (log,mark [8021p <0-7>|dscp <0-63>],
rule-precedence <1-5000>) {(rule-description <LINE>)}
```

<NETWORK-SERVICE-ALIAS-NAME>	Applies this deny rule to packets based on service protocols and ports specified in the network-service alias • <NETWORK-SERVICE-ALIAS-NAME> – Specify the network-service alias name (should be existing and configured). A network-service alias defines service protocols and ports to match. When used with an ACL, the network-service alias defines the service-specific components of the ACL deny rule. For more information on configuring network-service alias, see *alias*.
<SOURCE-IP/MASK>	Specifies the source IP address and mask (A.B.C.D/M) to match. Packets, matching the service protocols and ports specified in the network-service alias, received from the specified network are dropped.
<NETWORK-GROUP-ALIAS-NAME>	Applies a network-group alias to identify the source IP addresses. Packets, matching the service protocols and ports specified in the network-service alias, received from the addresses identified by the network-group alias are dropped. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured). A network-group alias defines a single or a range of addresses of devices, hosts, and networks. When used with an ACL, the network-group alias defines the network-specific component of the ACL rule (permit/deny).

any	Specifies the source as any source IP address. Packets, matching the service protocols and ports specified in the network-service alias, received from any source are dropped.
from-vlan <VLAN-ID>	Specifies a single VLAN or a range of VLANs as the match criteria. Packets, matching the service protocols and ports specified in the network-service alias, received from the specified VLAN(s) are dropped. • <VLAN-ID> – Specify the VLAN ID. To configure a range of VLANs, enter the start and end VLAN IDs separated by a hyphen (for example, 12-20). Use this option with WLANs and port ACLs.
host <SOURCE-HOST-IP>	Identifies a specific host (as the source to match) by its IP address. Packets, matching the service protocols and ports specified in the network-service alias, received from the specified host are dropped. • <SOURCE-HOST-IP> – Specify the source host's exact IP address in the A.B.C.D format.
<DEST-IP/MASK>	Specifies the destination IP address and mask (A.B.C.D/M) to match. Packets, matching the service protocols and ports specified in the network-service alias, addressed to the specified network are dropped.
any	Specifies the destination as any destination IP address. Packets, matching the service protocols and ports specified in the network-service alias, addressed to any destination are dropped.
host <DEST-HOST-IP>	Identifies a specific host (as the destination to match) by its IP address. Packets, matching the service protocols and ports specified in the network-service alias, addressed to the specified host are dropped. • <DEST-HOST-IP> – Specify the destination host's exact IP address in the A.B.C.D format.
<NETWORK-GROUP-ALIAS-NAME>	Applies a network-group alias to identify the destination IP addresses. Packets, matching the service protocols and ports specified in the network-service alias, destined for the addresses identified by the network-group alias are dropped. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured).
log	Logs all deny events matching this entry. If a source and/or destination IP address is matched (i.e. if any specified type of packet is received from a specified IP address and/or is destined for a specified IP address), an event is logged.
mark [8021p <0-7>| dscp <0-63>]	Specifies packets to mark • 8021p <0-7> – Marks packets by modifying 802.1.p VLAN user priority • dscp <0-63> – Marks packets by modifying DSCP TOS bits in the header
rule-precedence <1-5000> rule-description <LINE>	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Assigns a precedence for this deny rule • <1-5000> – Specify a value from 1 - 5000. Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • rule-description – Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

```
deny icmp [<SOURCE-IP/MASK>|<NETWORK-GROUP-NAME>|any|from-vlan <VLAN-ID>|
host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-NAME>|any|host
<DEST-HOST-IP>]
(<ICMP-TYPE> <ICMP-CODE>,log,rule-precedence <1-5000>) {(rule-description
<LINE>)}
```

icmp	Applies this deny rule to *Internet Control Message Protocol* (ICMP) packets only
<SOURCE-IP/MASK>	Specifies the source IP address and mask (A.B.C.D/M) to match. ICMP packets received from the specified sources are dropped.
<NETWORK-GROUP-ALIAS-NAME>	Applies a network-group alias to identify the source IP addresses. ICMP packets received from the addresses identified by the network-group alias are dropped. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured).
any	Specifies the source as any IP address. ICMP packets received from any source are dropped.

from-vlan <VLAN-ID>	Specifies a single VLAN or a range of VLANs as the match criteria. ICMP packets received from the VLANs identified here are dropped. • <VLAN-ID> – Specify the VLAN ID. To configure a range of VLANs, enter the start and end VLAN IDs separated by a hyphen (for example, 12-20). Use this option with WLANs and port ACLs.
host <SOURCE-HOST-IP>	Identifies a specific host (as the source to match) by its IP address. ICMP packets received from the specified host are dropped. • <SOURCE-HOST-IP> – Specify the source host's exact IP address in the A.B.C.D format.
<DEST-IP/MASK>	Specifies the destination IP address and mask (A.B.C.D/M) to match. ICMP packets addressed to specified destinations are dropped.
<NETWORK-GROUP-ALIAS-NAME>	Applies a network-group alias to identify the destination IP addresses. ICMP packets destined for addresses identified by the network-group alias are dropped. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured).
any	Specifies the destination as any IP address. ICMP packets addressed to any destination are dropped.
host <DEST-HOST-IP>	Identifies a specific host (as the destination to match) by its IP address. ICMP packets addressed to the specified host are dropped. • <DEST-HOST-IP> – Specify the destination host's exact IP address in the A.B.C.D format.
<ICMP-TYPE>	Defines the ICMP packet type For example, an ICMP type 0 indicates it is an ECHO REPLY, and type 8 indicates it is an ECHO.
<ICMP-CODE>	Defines the ICMP message type For example, an ICMP code 3 indicates "Destination Unreachable", code 1 indicates "Host Unreachable", and code 3 indicates "Port Unreachable." After specifying the source and destination IP address(es), the ICMP message type, and the ICMP code, specify the action taken in case of a match.
log	Logs all deny events matching this entry. If a source and/or destination IP address is matched (i.e. a ICMP packet is received from a specified IP address and/or is destined for a specified IP address), an event is logged.
rule-precedence <1-5000> rule-description <LINE>	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Assigns a precedence for this deny rule • <1-5000> – Specify a value from 1 - 5000. • rule-description – Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

```
deny ip [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>|
host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|host
<DEST-HOST-IP>] (log,rule-precedence <1-5000>) {(rule-description <LINE>)}
```

ip	Applies this deny rule to IP packets only
<SOURCE-IP/MASK>	Specifies the source IP address and mask (A.B.C.D/M) to match. IP packets received from the specified networks are dropped.
<NETWORK-GROUP-ALIAS-NAME>	Applies a network-group alias to identify the source IP addresses. IP packets received from the addresses identified by the network-group alias are dropped. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured).
any	Specifies the source as any IP address. IP packets received from any source are dropped.
from-vlan <VLAN-ID>	Specifies a single VLAN or a range of VLANs as the match criteria. IP packets received from the specified VLANs are dropped. • <VLAN-ID> – Specify the VLAN ID. To configure a range of VLAN IDs, enter the start and end VLAN IDs separated by a hyphen (for example, 12-20). Use this option with WLANs and port ACLs.

host <SOURCE-HOST-IP>	Identifies a specific host (as the source to match) by its IP address. IP packets received from the specified host are dropped. • <SOURCE-HOST-IP> – Specify the source host's exact IP address in the A.B.C.D format.
<DEST-IP/MASK>	Specifies the destination IP address and mask (A.B.C.D/M) to match. IP packets addressed to the specified networks are dropped.
any	Specifies the destination as any IP address. IP packets addressed to any destination are dropped.
host <DEST-HOST-IP>	Identifies a specific host (as the destination to match) by its IP address. IP packets addressed to the specified host are dropped. • <DEST-HOST-IP> – Specify the destination host's exact IP address in the A.B.C.D format.
<NETWORK-GROUP-ALIAS-NAME>	Applies a network-group alias to identify the source IP addresses. IP packets destined for addresses identified by the network-group alias are dropped. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured).
log	Logs all deny events matching this entry. If a source and/or destination IP address is matched (i.e. a IP packet is received from a specified IP address and/or is destined for a specified IP address), an event is logged.
rule-precedence <1-5000> rule-description <LINE>	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Assigns a precedence for this deny rule • <1-5000> – Specify a value from 1 - 5000. Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • rule-description – Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

```
deny proto [<PROTOCOL-NUMBER>|<PROTOCOL-NAME>|eigrp|gre|igmp|igp|ospf|vrrp]
[<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>|
host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|
host <DEST-HOST-IP>] (log,rule-precedence <1-5000>) {(rule-description
<LINE>)}
```

proto	Configures the ACL for additional protocols Additional protocols (other than IP, ICMP, TCP, and UDP) must be configured using this parameter
<PROTOCOL-NUMBER>	Filters protocols using their *Internet Assigned Numbers Authority* (IANA) protocol number • <PROTOCOL-NUMBER> – Specify the protocol number.
<PROTOCOL-NAME>	Filters protocols using their IANA protocol name • <PROTOCOL-NAME> – Specify the protocol name.
eigrp	Identifies the *Enhanced Internet Gateway Routing Protocol* (EIGRP) protocol (number 88) EIGRP enables routers to maintain copies of neighbors' routing tables. Routers use this information to determine the fastest route to a destination. When a router fails to find a route in its stored route tables, it sends a query to neighbors who in turn query their neighbors till a route is found. EIGRP also enables routers to inform neighbors of changes in their routing tables.
gre	Identifies the *General Routing Encapsulation* (GRE) protocol (number 47) GRE is a tunneling protocol that enables transportation of protocols (IP, IPX, DEC net, etc.) over an IP network. GRE encapsulates the packet at the source and removes the encapsulation at the destination.
igmp	Identifies the *Internet Group Management Protocol* (IGMP) protocol (number 2) IGMP establishes and maintains multicast group memberships to interested members. Multicasting allows a networked computer to send content to multiple computers who have registered to receive the content. IGMP snooping is for listening to IGMP traffic between an IGMP host and routers in the network to maintain a map of the links that require multicast streams. Multicast traffic is filtered out for those links which do not require them.

igp	Identifies any private internal gateway (primarily used by CISCO for their IGRP) (number 9) IGP enables exchange of information between hosts and routers within a managed network. The most commonly used *interior gateway protocol* (IGP) protocols are: *Routing Information Protocol* (RIP) and *Open Shortest Path First* (OSPF)
ospf	Identifies the OSPF protocol (number 89) OSPF is a link-state *interior gateway protocol* (IGP). OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighbor routers and constructs a network topology. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets.
vrrp	Identifies the *Virtual Router Redundancy Protocol* (VRRP) protocol (number 112) VRRP allows a pool of routers to be advertized as a single virtual router. This virtual router is configured by hosts as their default gateway. VRRP elects a master router, from this pool, and assigns it a virtual IP address. The master router routes and forwards packets to hosts on the same subnet. When the master router fails, one of the backup routers is elected as the master and its IP address is mapped to the virtual IP address.
<SOURCE-IP/MASK>	Specifies the source IP address and mask (A.B.C.D/M) to match. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the specified sources are dropped.
<NETWORK-GROUP-ALIAS -NAME>	Applies a network-group alias to identify the source IP addresses. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the sources defined in the network-group alias are dropped. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured).
any	Specifies the source as any IP address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from any source are dropped.
from-vlan <VLAN-ID>	Specifies a single VLAN or a range of VLANs as the match criteria. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the VLANs identified here are dropped. • <VLAN-ID> – Specify the VLAN ID. A range of VLANs is represented by the start and end VLAN IDs separated by a hyphen (for example, 12-20). Use this option with WLANs and port ACLs.
host <SOURCE-HOST-IP>	Identifies a specific host (as the source to match) by its IP address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the specified host are dropped. • <SOURCE-HOST-IP> – Specify the source host's exact IP address in the A.B.C.D format.
<DEST-IP/MASK>	Specifies the destination IP address and mask (A.B.C.D/M) to match. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to the specified destinations are dropped.
any	Specifies the destination as any IP address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to any destination are dropped.
host <DEST-HOST-IP>	Identifies a specific host (as the destination to match) by its IP address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addresses to the specified host are dropped. • <SOURCE-HOST-IP> – Specify the destination host's exact IP address in the A.B.C.D format.
<NETWORK-GROUP-ALIAS -NAME>	Applies a network-group alias to identify the destination IP addresses. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to the destinations identified in the network-group alias are dropped. • <NETWORK-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured). After specifying the source and destination IP address(es), specify the action taken in case of a match.

log	Logs all deny events matching this entry. If a source and/or destination IP address is matched (i.e. a packet (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) is received from a specified IP address and/or is destined for a specified IP address), an event is logged.
rule-precedence <1-5000> rule-description <LINE>	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Assigns a precedence for this deny rule • <1-5000> – Specify a value from 1 - 5000. Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • rule-description – Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

```
deny [tcp|udp] [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan
<VLAN-ID>|
host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|eq
<SOURCE-PORT>|
host <DEST-HOST-IP>|range <START-PORT> <END-PORT>] [eq
[<1-65535>|<SERVICE-NAME>|bgp|
dns|ftp|ftp-data|gopher|https|ldap|nntp|ntp|pop3|sip|smtp|ssh|telnet|tftp|www
]|
range <START-PORT> <END-PORT>] (log,rule-precedence <1-5000>)
{(rule-description <LINE>)}
```

tcp	Applies this deny rule to TCP packets only
udp	Applies this deny rule to UDP packets only
<SOURCE-IP/MASK>	This keyword is common to the 'tcp' and 'udp' parameters. Specifies the source IP address and mask (A.B.C.D/M) to match. TCP/UDP packets received from the specified sources are dropped.
<NETWORK-GROUP-ALIAS-NAME>	This keyword is common to the 'tcp' and 'udp' parameters. Applies a network-group alias to identify the source IP addresses. TCP/UDP packets received from the VLANs identified here are dropped. • <NETWORK-ALIAS-GROUP-NAME> – Specify the network-group alias name (should be existing and configured). After specifying the source and destination IP address(es), specify the action taken in case of a match.
any	This keyword is common to the 'tcp' and 'udp' parameters. Specifies the source as any IP address. TCP/UDP packets received from any source are dropped.
from-vlan <VLAN-ID>	This keyword is common to the 'tcp' and 'udp' parameters. Specifies a single VLAN or a range of VLANs as the match criteria. TCP/UDP packets received from the VLANs identified here are dropped. • <VLAN-ID> – Specify the VLAN ID. To configure a range of VLANs, enter the start and end VLAN IDs separated by a hyphen (for example, 12-20). Use this option with WLANs and port ACLs.
host <SOURCE-HOST-IP>	Identifies a specific host (as the source to match) by its IP address. TCP/UDP packets received from the specified host are dropped. • <SOURCE-HOST-IP> – Specify the source host's exact IP address in the A.B.C.D format.
<DEST-IP/MASK>	This keyword is common to the 'tcp' and 'udp' parameters. Sets the destination IP address and mask (A.B.C.D/M) to match. TCP/UDP packets addressed to the specified destinations are dropped.
any	This keyword is common to the 'tcp' and 'udp' parameters. Specifies the destination as any destination IP address. TCP/UDP packets received from any destination are dropped.
eq <SOURCE-PORT>	Identifies a specific source port • <SOURCE-PORT> – Specify the exact source port.

host <DEST-HOST-IP>	Identifies a specific host (as the destination to match) by its IP address. TCP/UDP packets addressed to the specified host are dropped. • <DEST-HOST-IP> – Specify the destination host's exact IP address in the A.B.C.D format.
<NETWORK-GROUP-ALIAS -NAME>	This keyword is common to the 'tcp' and 'udp' parameters. Applies a network-group alias to identify the destination IP addresses. TCP/UDP packets destined to the addresses identified in the network-group alias are dropped. • <NETWORK-ALIAS-GROUP-NAME> – Specify the network-group alias name (should be existing and configured).
range <START-PORT> <END-PORT>	Specifies a range of source ports • <START-PORT> – Specify the first port in the range. • <END-PORT> – Specify the last port in the range.
eq [<1-65535>| <SERVICE-NAME>| |bgp|dns|ftp| ftp-data|gopher| https|ldap|nntp|ntp| pop3|sip|smtp| ssh|telnet| tftp|www]	Identifies a specific destination or protocol port to match • <1-65535> – The destination port is designated by its number • <SERVICE-NAME> – Specifies the service name • bgp – The designated *Border Gateway Protocol* (BGP) protocol port (179) • dns – The designated *Domain Name System* (DNS) protocol port (53) • ftp – The designated *File Transfer Protocol* (FTP) protocol port (21) • ftp-data – The designated FTP data port (20) • gropher – The designated GROPHER protocol port (70) • https – The designated HTTPS protocol port (443) • ldap – The designated *Lightweight Directory Access Protocol* (LDAP) protocol port (389) • nntp – The designated *Network News Transfer Protocol* (NNTP) protocol port (119) • ntp – The designated *Network Time Protocol* (NTP) protocol port (123) • pop3 – The designated POP3 protocol port (110) Contd..
	• sip – The designated *Session Initiation Protocol* (SIP) protocol port (5060) • smtp – The designated *Simple Mail Transfer Protocol* (SMTP) protocol port (25) • ssh – The designated *Secure Shell* (SSH) protocol port (22) • telnet – The designated Telnet protocol port (23) • tftp – The designated *Trivial File Transfer Protocol* (TFTP) protocol port (69) • www – The designated www protocol port (80)
range <START-PORT> <END-PORT>	Specifies a range of destination ports • <START-PORT> – Specify the first port in the range. • <END-PORT> – Specify the last port in the range.
log	Logs all deny events matching this entry. If a source and/or destination IP address or port is matched (i.e. a TCP/UDP packet is received from a specified IP address and/or is destined for a specified IP address), an event is logged.
rule-precedence <1-5000> rule-description <LINE>	The following keywords are recursive and common to all of the above: • rule-precedence – Assigns a precedence for this deny rule • <1-5000> – Specify a value from 1 - 5000. Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • rule-description – Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

Usage Guidelines:

Use this command to deny traffic between networks/hosts based on the protocol type selected in the access list configuration. The following protocols are supported:

- IP
- ICMP

- TCP
- UDP
- PROTO (any Internet protocol other than TCP, UDP, and ICMP)

The last *access control entry* (ACE) in the access list is an implicit deny statement.

Whenever the interface receives the packet, its content is checked against the ACEs in the ACL. It is allowed or denied based on the ACL configuration.

- Filtering TCP/UDP allows you to specify port numbers as filtering criteria
- Select ICMP as the protocol to allow or deny ICMP packets. Selecting ICMP filters ICMP packets based on ICMP type and code.

NOTE
The log option is functional only for router ACL's. The log option displays an informational logging message about the packet that matches the entry sent to the console.

Example

```
rfs7000-37FABE(config-ip-acl-test)#deny proto vrrp any any log rule-precedence
600
rfs7000-37FABE(config-ip-acl-test)#deny proto ospf any any log rule-precedence
650

rfs7000-37FABE(config-ip-acl-test)#show context
ip access-list test
 deny proto vrrp any any log rule-precedence 600
 deny proto ospf any any log rule-precedence 650
rfs7000-37FABE(config-ip-acl-test)#
```

Using aliases in IP access list.

The following examples show the usage of network-group aliases:

```
rfs4000-229D58(config)#ip access-list bar
```

Example 1:

```
rfs4000-229D58(config-ip-acl-bar)#permit ip $foo any rule-precedence 10
```

Example 2

```
rfs4000-229D58(config-ip-acl-bar)#permit tcp 192.168.100.0/24 $foobar eq ftp
rule-precedence 20
```

Example 3

```
rfs4000-229D58(config-ip-acl-bar)#deny ip $guest  $lab rule-precedence 30
```

- In example1, network-group alias **$foo** is used as a source
- In example 2, network-group alias **$foobar** is used as a destination
- In example 3, network-group aliases **$guest** and **$lab** are used as source and destination respectively.

The following examples show the usage of network-service aliases:

Example 4

```
rfs4000-229D58(config-ip-acl-bar)# permit $kerberos 10.60.20.0/24
$kerberos-servers log rule-precedence 40
```

Example 5

```
rfs4000-229D58(config-ip-acl-bar)#permit $Tandem 10.60.20.0/24
$Tandem-servers log rule-precedence 50
```

In examples 4, and 5:

- The network-service aliases (**$kerberos** and **$Tandem**) define the destination protocol-port combinations
- The source network is **10.60.20.0/24**
- The destination network-address combinations are defined by the network-group aliases (**$kerberos-servers** and **$Tandem-servers**)

Related Commands:

no	Removes a specified IP deny access rule
alias	Creates and configures aliases (network, VLAN, and service)

disable

ip-access-list

Disables an existing deny or permit rule without removing it from the ACL. A disabled rule is inactive and is not used to filter packets.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
disable [deny|permit] [<NETWORK-SERVICE-ALIAS-NAME>|icmp|ip|proto|tcp|udp]

disable [deny|permit] [<NETWORK-SERVICE-ALIAS-NAME>|icmp|ip|proto
<PROTOCOL-OPTIONS>|
          tcp|udp] [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan
<VLAN-ID>|
          host <SOURCE-HOST-IP>]
[<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|
          host <DEST-HOST-IP>] (log,mark [8021p <0-7>|dscp
<0-63>],rule-precedence)
```

Parameters

```
disable [deny|permit] [<NETWORK-SERVICE-ALIAS-NAME>|icmp|ip|
proto <PROTOCOL-OPTIONS>|tcp|udp]
[<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|
from-vlan <VLAN-ID>|host <SOURCE-HOST-IP>]
[<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|
any|host <DEST-HOST-IP>] (log,mark [8021p <0-7>|dscp <0-63>],rule-precedence)
```

disable [deny|permit]	Disables a deny or permit access rule without removing it from the ACL Provide the exact values used to configure the deny or permit rule.
<NETWORK-SERVICE-ALIAS-NAME>	Specifies the network-service alias, identified by the <NETWORK-SERVICE-ALIAS-NAME> keyword, associated with the deny/permit rule
icmp	Disables a rule applicable to ICMP packets only
ip	Disables a rule applicable to IP packets only
proto <PROTOCOL-OPTIONS>	Disables a rule applicable to any Internet protocol other than TCP, UDP, or ICMP packets • <PROTOCOL-OPTIONS> – Identify the Internet protocol using the options available.
tcp	Disables a rule applicable to TCP packets only
udp	Disables a rule applicable to UDP packets only After specifying the packet type, specify the source and destination devices and network address(es) to match.
<SOURCE-IP/MASK>	Specify the source IP address and mask in the A.B.C.D/M format.
<NETWORK-GROUP-ALIAS-NAME>	Specifies the network-group alias, identified by the <NETWORK-GROUP-ALIAS-NAME> keyword, associated with this deny/permit rule
any	Select 'any' if the rule is applicable to any source IP address.
from-vlan <VLAN-ID>	Specify the VLAN IDs.
host <SOURCE-HOST-IP>	Specify the source host's exact IP address.
<DEST-IP/MASK>	Specify the destination IP address and mask in the A.B.C.D/M format.
<NETWORK-GROUP-ALIAS-NAME>	Specifies the network-group alias, identified by the <NETWORK-GROUP-ALIAS-NAME> keyword, associated with this deny/permit rule
any	Select 'any' if the rule is applicable to any destination IP address.
host <DEST-HOST-IP>	Specify the destination host's exact IP address.
log	Select log, if the rule has been configured to log records in case of a match.
mark [8021p <0-7>| dscp <0-63>]	Specifies packets to mark • 8021p <0-7> – Marks packets by modifying 802.1.p VLAN user priority • dscp <0-63> – Marks packets by modifying DSCP TOS bits in the header
rule-precedence <1-5000>	Specify the rule precedence. The deny or permit rule with the specified precedence is disabled. To enable a disabled rule, enter the rule again without the 'disable' keyword. The *no* > *disable* command removes a disabled rule from the ACL.

Example

```
The following example shows the 'auto-tunnel-acl' settings before the disable
command is executed:

rfs7000-37FABE(config-ip-acl-auto-tunnel-acl)#show context
ip access-list auto-tunnel-acl
 permit ip host 200.200.200.99 30.30.30.1/24 rule-precedence 2
 permit ip host 200.200.200.99 any rule-precedence 3
rfs7000-37FABE(config-ip-acl-auto-tunnel-acl)#
```

```
rfs7000-37FABE(config-ip-acl-auto-tunnel-acl)#disable permit ip host
200.200.200.99 any rule-precedence 3
rfs7000-37FABE(config-ip-acl-auto-tunnel-acl)#

The following example shows the ‘auto-tunnel-acl’ settings after the disable
command is executed:

rfs7000-37FABE(config-ip-acl-auto-tunnel-acl)#show context
ip access-list auto-tunnel-acl
 permit ip host 200.200.200.99 30.30.30.1/24 rule-precedence 2
 disable permit ip host 200.200.200.99 any rule-precedence 3
rfs7000-37FABE(config-ip-acl-auto-tunnel-acl)#

rfs4000-229D58(config-ip-acl-test)#deny icmp any any log rule-precedence 1

rfs4000-229D58(config-ip-acl-test)#show context
ip access-list test
 deny icmp any any rule-precedence 1
rfs4000-229D58(config-ip-acl-test)#

rfs4000-229D58(config-ip-acl-test)#disable deny icmp any any rule-precedence 1

rfs4000-229D58(config-ip-acl-test)#show context
ip access-list test
 disable deny icmp any any rule-precedence 1
rfs4000-229D58(config-ip-acl-test)#
```

Related Commands:

no	Enables a disabled deny or permit rule
deny	Creates a new deny access rule or modifies an existing rule
permit	Creates a new permit access rule or modifies an existing rule
alias	Creates and configures a aliases (network, VLAN, and service)

insert

ip-access-list

Enables the insertion of a rule in an IP ACL without overwriting or replacing an existing rule having the same precedence

The insert option allows a new rule to be inserted within a IP access list. Consider an IP ACL consisting of rules having precedences 1, 2, 3, 4, 5, and 6. You want to insert a new rule with precedence 4, without overwriting the existing precedence 4 rule. Using the insert option inserts the new rule prior to the existing one. The existing precedence 4 rule’s precedence changes to 5, and the change cascades down the list of rules within the ACL. That means rule 5 becomes rule 6, and rule 6 becomes rule 7.

NOTE
NOT using *insert* when creating a new rule having the same precedence as an existing rule, overwrites the existing rule.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
insert [deny|permit] <PARAMETERS> (log,mark [8021p <0-7>|dscp <0-63>],
          rule-precedence <1-5000>) {(rule-description <LINE>)}
```

Parameters

```
insert [deny|permit] <PARAMETERS> (log,mark [8021p <0-7>|dscp <0-63>],
rule-precedence <1-5000>) {(rule-description <LINE>)}
```

[deny|permit]	Inserts a deny or a permit rule within an IP ACL
<PARMETERS>	Provide the match criteria for this deny/permit rule. Packets will be filtered based on the criteria set here. For more information on the deny rule, see *deny*. For more information on the permit rule, see *permit*.
log	After specifying the match criteria, specify the action taken for filtered packets Logs all deny/permit events matching this entry. If a source and/or destination IP address is matched an event is logged.
mark [8021p <0-7>| dscp <0-63>]	Specifies packets to mark • 8021p <0-7> – Marks packets by modifying 802.1.p VLAN user priority • dscp <0-63> – Marks packets by modifying DSCP TOS bits in the header
rule-precedence <1-5000> rule-description <LINE>	Assigns a precedence for this deny/permit rule • <1-5000> – Specify a value from 1 - 5000. Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • rule-description – Optional. Configures a description for this new rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

NOTE
The log option is functional only for router ACL's. The log option displays an informational logging message about the packet that matches the entry sent to the console.

Example

```
rfs4000-229D58(config-ip-acl-test)#deny tcp from-vlan 1 any any
rule-precedence 1

rfs4000-229D58(config-ip-acl-test)#permit icmp any host 192.168.13.7 1 1
rule-precedence 2

rfs4000-229D58(config-ip-acl-test)#show context
ip access-list test
 deny tcp from-vlan 1 any any rule-precedence 1
 permit icmp any host 192.168.13.7 1 1 rule-precedence 2
rfs4000-229D58(config-ip-acl-test)#
```

```
In the following example a new rule is inserted between the rules having
precedences 1 and 2. The precedence of the existing precedence ‘2’ rule
changes to precedence 3.

rfs4000-229D58(config-ip-acl-test)#insert deny ip any any rule-precedence 2

rfs4000-229D58(config-ip-acl-test)#show context
ip access-list test
 deny tcp from-vlan 1 any any rule-precedence 1
 deny ip any any rule-precedence 2
 permit icmp any host 192.168.13.7 1 1 rule-precedence 3
rfs4000-229D58(config-ip-acl-test)#
```

Related Commands:

alias	Creates and configures aliases (network, VLAN, and service)

no

ip-access-list

Removes a deny, permit, or disable rule

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no [deny|disable|permit]

no [deny|permit] [<NETWORK-SERVICE-ALIAS-NAME>|icmp|ip|proto|tcp|udp]
          <RULE-PARAMETERS>

no disable [deny|permit] [<NETWORK-SERVICE-ALIAS-NAME>|icmp|ip|proto|tcp|udp]
          <RULE-PARAMETERS>
```

Parameters

```
no [deny|permit] <NETWORK-SERVICE-ALIAS-NAME>icmp|ip|proto|tcp|udp]
<RULE-PARAMETERS>
```

no [deny|permit]	Removes a deny or permit rule from the selected IP access list
<NETWORK-SERVICE-ALIAS-NAME>	Removes a deny or permit rule applicable to the specified network-service alias • <NETWORK-SERVICE-ALIAS-NAME> – Specify the network-service alias name (should be existing and configured).
icmp	Removes a deny or permit rule applicable to ICMP packets only
ip	Removes a deny or permit rule applicable to IP packets only
proto	Removes a deny or permit rule applicable to protocols (other than IP, ICMP, TCP, and UDP)
[tcp|udp]	Removes a deny or permit rule applicable to TCP/UDP packets

<RULE-PARAMETERS>	Enter the exact parameters used when configuring the rule.
rule-precedence <1-5000> rule-description <LINE>	Specify the precedence assigned to this deny/permit rule. • rule-description – Optional. Specify the rule description. The system removes the rule from the selected ACL.

```
no disable [deny|permit] [<NETWORK-SERVICE-ALIAS-NAME>|icmp|ip|proto|tcp|udp]
<RULE-PARAMETERS>
```

no disabled [deny|permit]	Removes a disabled deny or permit rule from the selected IP access list
<NETWORK-SERVICE-ALIAS-NAME>	Removes a disabled deny or permit rule applicable to the specified network-service alias • <NETWORK-SERVICE-ALIAS-NAME> – Specify the network-service alias name (should be existing and configured).
icmp	Removes a disabled deny or permit rule applicable to ICMP packets only
ip	Removes a disabled deny or permit rule applicable to IP packets only
proto	Removes a disabled deny or permit rule applicable to protocols (other than IP, ICMP, TCP, and UDP)
[tcp|udp]	Removes a disabled deny or permit rule applicable to TCP/UDP packets
<RULE-PARAMETERS>	Enter the exact parameters used when configuring the rule.
rule-precedence <1-5000> rule-description <LINE>	Specify the precedence assigned to this disabled deny/permit rule. • rule-description – Optional. Specify the rule description. The system removes the disabled rule from the selected ACL.

Usage Guidelines:

```
Removes an access list control entry. Provide the rule-precedence value when
using the no command.
```

Example

```
The following example shows the ACL ‘test’ settings before the ‘no’ commands
are executed:

rfs7000-37FABE(config-ip-acl-test)#show context
ip access-list test
 deny proto vrrp any any log rule-precedence 600
 deny proto ospf any any log rule-precedence 650
rfs7000-37FABE(config-ip-acl-test)#

rfs7000-37FABE(config-ip-acl-test)#no deny proto vrrp any any rule-precedence
600
rfs7000-37FABE(config-ip-acl-test)#no deny proto ospf any any rule-precedence
650

The following example shows the ACL ‘test’ settings after the ‘no’ commands
are executed:

rfs7000-37FABE(config-ip-acl-test)#show context
ip access-list test
rfs7000-37FABE(config-ip-acl-test)#
```

Related Commands:

deny	Creates a deny access rule

disable	Disables a deny or permit rule within an IP ACL
permit	Creates a permit access rule

permit

ip-access-list

Creates a permit rule that marks packets (from a specified source IP and/or to a specified destination IP) for forwarding. You can also use this command to modify an existing permit rule.

NOTE
Use a decimal value representation to implement a `permit/deny` designation for a packet. The command set for IP ACLs provides the hexadecimal values for each listed EtherType. Use the decimal equivalent of the EtherType listed for any other EtherType.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
permit [<NETWORK-SERVICE-ALIAS-NAME>|icmp|ip|proto|tcp|udp]

permit <NETWORK-SERVICE-ALIAS-NAME>
[<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|
          from-vlan <VLAN-ID>|host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|any|host
<DEST-HOST-IP>|
          <NETWORK-GROUP-ALIAS-NAME>] (log,mark [8021p <0-7>|dscp <0-63>],
          rule-precedence <1-5000>) {(rule-description <LINE>)}

permit icmp [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan
<VLAN-ID>|
          host <SOURCE-HOST-IP>]
[<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|
          host <DEST-HOST-IP>] (<ICMP-TYPE> <ICMP-CODE>,log,rule-precedence
<1-5000>)
          {(rule-description <LINE>)}

permit ip [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan
<VLAN-ID>|
          host <SOURCE-HOST-IP>]
[<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|
          host <DEST-HOST-IP>] (log,rule-precedence <1-5000>) {(
rule-description <LINE>)}
```

```
permit proto [<PROTOCOL-NUMBER>|<PROTOCOL-NAME>|eigrp|gre|igmp|igp|ospf|vrrp]
          [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan
<VLAN-ID>|
          host <SOURCE-HOST-IP>]
[<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|
          host <DEST-HOST-IP>] (log,rule-precedence <1-5000>)
{(rule-description <LINE>)}

permit [tcp|udp] [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan
<VLAN-ID>|
          host <SOURCE-HOST-IP>]
[<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|
          eq <SOURCE-PORT>|host <DEST-HOST-IP>|range <START-PORT> <END-PORT>]
          [eq
[<1-65535>|<SERVICE-NAME>|bgp|dns|ftp|ftp-data|gopher|https|ldap|nntp|ntp|pop
3|
          sip|smtp|ssh|telnet|tftp|www]|range <START-PORT> <END-PORT>]
          (log,rule-precedence <1-5000>) {(rule-description <LINE>)}
```

Parameters

```
permit <NETWORK-SERVICE-ALIAS-NAME>
[<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>|host
<SOURCE-HOST-IP>] [<DEST-IP/MASK>|any|host
<DEST-HOST-IP>|<NETWORK-GROUP-ALIAS-NAME>] (log,mark [8021p <0-7>|dscp
<0-63>],
rule-precedence <1-5000>) {(rule-description <LINE>)}
```

<NETWORK-SERVICE-ALIAS-NAME>	Applies this permit rule to packets based on service protocols and ports specified in the network-service alias • <NETWORK-SERVICE-ALIAS-NAME> – Specify the network-service alias name (should be existing and configured). A network-service alias defines service protocols and ports to match. When used with an ACL, the network-service alias defines the service-specific components of the ACL permit rule. For more information on configuring network-service alias, see *alias*.
<SOURCE-IP/MASK>	Specifies the source IP address and mask (A.B.C.D/M) to match. Packets, matching the service protocols and ports specified in the network-service alias, received from the specified network are permitted.
<NETWORK-GROUP-ALIAS-NAME>	Applies a network-group alias to identify the source IP addresses. Packets, matching the service protocols and ports specified in the network-service alias, received from the addresses identified by the network-group alias are permitted. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured). A network-group alias defines a single or a range of addresses of devices, hosts, and networks. When used with an ACL, the network-group alias defines the network-specific component of the ACL rule (permit/deny).
any	Specifies the source as any source IP address. Packets, matching the service protocols and ports specified in the network-service alias, received from any source are permitted.
from-vlan <VLAN-ID>	Specifies a single VLAN or a range of VLANs as the match criteria. Packets, matching the service protocols and ports specified in the network-service alias, received from the specified VLAN(s) are permitted. • <VLAN-ID> – Specify the VLAN ID. To configure a range of VLANs, enter the start and end VLAN IDs separated by a hyphen (for example, 12-20). Use this option with WLANs and port ACLs.
host <SOURCE-HOST-IP>	Identifies a specific host (as the source to match) by its IP address. Packets, matching the service protocols and ports specified in the network-service alias, received from the specified host are permitted. • <SOURCE-HOST-IP> – Specify the source host's exact IP address in the A.B.C.D format.
<DEST-IP/MASK>	Specifies the destination IP address and mask (A.B.C.D/M) to match. Packets, matching the service protocols and ports specified in the network-service alias, addressed to the specified network are permitted.

any	Specifies the destination as any destination IP address. Packets, matching the service protocols and ports specified in the network-service alias, addressed to any destination are permitted.
host <DEST-HOST-IP>	Identifies a specific host (as the destination to match) by its IP address. Packets, matching the service protocols and ports specified in the network-service alias, addressed to the specified host are permitted. • <DEST-HOST-IP> – Specify the destination host's exact IP address in the A.B.C.D format.
<NETWORK-GROUP-ALIAS-NAME>	Applies a network-group alias to identify the destination IP addresses. Packets, matching the service protocols and ports specified in the network-service alias, destined for the addresses identified by the network-group alias are permitted. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured).
log	Logs all permit events matching this entry. If a source and/or destination IP address is matched (i.e. if any specified type of packet is received from a specified IP address and/or is destined for a specified IP address), an event is logged.
mark [8021p <0-7>| dscp <0-63>]	Specifies packets to mark • 8021p <0-7> – Marks packets by modifying 802.1.p VLAN user priority • dscp <0-63> – Marks packets by modifying DSCP TOS bits in the header
rule-precedence <1-5000> rule-description <LINE>	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Assigns a precedence for this permit rule • <1-5000> – Specify a value from 1 - 5000. Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • rule-description – Optional. Configures a description for this permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

```
permit icmp [<SOURCE-IP/MASK>|<NETWORK-GROUP-NAME>|any|from-vlan <VLAN-ID>|
host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-NAME>|any|host
<DEST-HOST-IP>]
(<ICMP-TYPE> <ICMP-CODE>,log,rule-precedence <1-5000>) {(rule-description
<LINE>)}
```

icmp	Applies this permit rule to ICMP packets only
<SOURCE-IP/MASK>	Specifies the source IP address and mask (A.B.C.D/M) to match. ICMP packets received from the specified sources are permitted.
<NETWORK-GROUP-ALIAS-NAME>	Applies a network-group alias to identify the source IP addresses. ICMP packets received from the addresses identified by the network-group alias are permitted. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured).
any	Specifies the source as any source IP address. ICMP packets received from any source are permitted.
from-vlan <VLAN-ID>	Specifies a single VLAN or a range of VLANs as the match criteria. ICMP packets received from the VLANs identified here are permitted. • <VLAN-ID> – Specify the VLAN ID. To configure a range of VLANs, enter the start and end VLAN IDs separated by a hyphen (for example, 12-20). Use this option with WLANs and port ACLs.
host <SOURCE-HOST-IP>	Identifies a specific host (as the source to match) by its IP address. ICMP packets received from the specified host are permitted. • <SOURCE-HOST-IP> – Specify the source host's exact IP address in the A.B.C.D format.
<DEST-IP/MASK>	Specifies the destination IP address and mask (A.B.C.D/M) to match. ICMP packets addressed to specified destinations are permitted.

<NETWORK-GROUP-ALIAS-NAME>	Applies a network-group alias to identify the destination IP addresses. ICMP packets destined for addresses identified by the network-group alias are permitted. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured).
any	Specifies the destination as any destination IP address. ICMP packets addressed to any destination are permitted.
host <DEST-HOST-IP>	Identifies a specific host (as the destination to match) by its IP address. ICMP packets addressed to the specified host are permitted. • <DEST-HOST-IP> – Specify the destination host's exact IP address in the A.B.C.D format.
<ICMP-TYPE>	Defines the ICMP packet type For example, an ICMP type 0 indicates it is an ECHO REPLY, and type 8 indicates it is an ECHO.
<ICMP-CODE>	Defines the ICMP message type For example, an ICMP code 3 indicates "Destination Unreachable", code 1 indicates "Host Unreachable", and code 3 indicates "Port Unreachable." After specifying the source and destination IP address(es), the ICMP message type, and the ICMP code, specify the action taken in case of a match.
log	Logs all permit events matching this entry. If a source and/or destination IP address is matched (i.e. a ICMP packet is received from a specified IP address and/or is destined for a specified IP address), an event is logged.
rule-precedence <1-5000> rule-description <LINE>	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Assigns a precedence for this permit rule • <1-5000> – Specify a value from 1 - 5000. Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • rule-description – Optional. Configures a description for this permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

```
permit ip [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan
<VLAN-ID>|
host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|host
<DEST-HOST-IP>] (log,rule-precedence <1-5000>) {(rule-description <LINE>)}
```

ip	Applies this permit rule to IP packets only
<SOURCE-IP/MASK>	Specifies the source IP address and mask (A.B.C.D/M) to match. IP packets received from the specified networks are permitted.
<NETWORK-GROUP-ALIAS-NAME>	Applies a network-group alias to identify the source IP addresses. IP packets received from the addresses identified by the network-group alias are permitted. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured).
any	Specifies the source as any source IP address. IP packets received from any source are permitted.
from-vlan <VLAN-ID>	Specifies a single VLAN or a range of VLANs as the match criteria. IP packets received from the specified VLANs are permitted. • <VLAN-ID> – Specify the VLAN ID. To configure a range of VLAN IDs, enter the start and end VLAN IDs separated by a hyphen (for example, 12-20). Use this option with WLANs and port ACLs.
host <SOURCE-HOST-IP>	Identifies a specific host (as the source to match) by its IP address. IP packets received from the specified host are permitted. • <SOURCE-HOST-IP> – Specify the source host's exact IP address in the A.B.C.D format.
<DEST-IP/MASK>	Specifies the destination IP address and mask (A.B.C.D/M) to match. IP packets addressed to the specified networks are permitted.

any	Specifies the destination as any destination IP address. IP packets addressed to any destination are permitted.
host <DEST-HOST-IP>	Identifies a specific host (as the destination to match) by its IP address. IP packets addressed to the specified host are permitted. • <DEST-HOST-IP> – Specify the destination host's exact IP address in the A.B.C.D format.
<NETWORK-GROUP-ALIAS-NAME>	Applies a network-group alias to identify the source IP addresses. IP packets destined for addresses identified by the network-group alias are permitted. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured).
log	Logs all permit events matching this entry. If a source and/or destination IP address is matched (i.e. a IP packet is received from a specified IP address and/or is destined for a specified IP address), an event is logged.
rule-precedence <1-5000> rule-description <LINE>	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Assigns a precedence for this permit rule • <1-5000> – Specify a value from 1 - 5000. Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • rule-description – Optional. Configures a description for this permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

```
permit proto [<PROTOCOL-NUMBER>|<PROTOCOL-NAME>|eigrp|gre|igmp|igp|ospf|vrrp]
[<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>|host
<SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|host
<DEST-HOST-IP>] (log,rule-precedence <1-5000>) {(rule-description <LINE>)}
```

proto	Configures the ACL for additional protocols Additional protocols (other than IP, ICMP, TCP, and UDP) must be configured using this parameter
<PROTOCOL-NUMBER>	Filters protocols using their IANA protocol number • <PROTOCOL-NUMBER> – Specify the protocol number.
<PROTOCOL-NAME>	Filters protocols using their IANA protocol name • <PROTOCOL-NAME> – Specify the protocol name.
eigrp	Identifies the EIGRP protocol (number 88) EIGRP enables routers to maintain copies of neighbors' routing tables. Routers use this information to determine the fastest route to a destination. When a router fails to find a route in its stored route tables, it sends a query to neighbors who in turn query their neighbors till a route is found. EIGRP also enables routers to inform neighbors of changes in their routing tables.
gre	Identifies the GRE protocol (number 47) GRE is a tunneling protocol that enables transportation of protocols (IP, IPX, DEC net, etc.) over an IP network. GRE encapsulates the packet at the source and removes the encapsulation at the destination.
igmp	Identifies the IGMP protocol (number 2) IGMP establishes and maintains multicast group memberships to interested members. Multicasting allows a networked computer to send content to multiple computers who have registered to receive the content. IGMP snooping is for listening to IGMP traffic between an IGMP host and routers in the network to maintain a map of the links that require multicast streams. Multicast traffic is filtered out for those links which do not require them.
igp	Identifies any private internal gateway (primarily used by CISCO for their IGRP) (number 9) IGP enables exchange of information between hosts and routers within a managed network. The most commonly used *interior gateway protocol* (IGP) protocols are: *Routing Information Protocol* (RIP) and *Open Shortest Path First* (OSPF)

ospf	Identifies the OSPF protocol (number 89) OSPF is a link-state *interior gateway protocol* (IGP). OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighbor routers and constructs a network topology. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets.
vrrp	Identifies the VRRP protocol (number 112) VRRP allows a pool of routers to be advertized as a single virtual router. This virtual router is configured by hosts as their default gateway. VRRP elects a master router, from this pool, and assigns it a virtual IP address. The master router routes and forwards packets to hosts on the same subnet. When the master router fails, one of the backup routers is elected as the master and its IP address is mapped to the virtual IP address.
<SOURCE-IP/MASK>	Specifies the source IP address and mask (A.B.C.D/M) to match. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the specified sources are permitted.
<NETWORK-GROUP-ALIAS -NAME>	Applies a network-group alias to identify the source IP addresses. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the sources defined in the network-group alias are permitted. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured).
any	Specifies the source as any IP address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from any source are permitted.
from-vlan <VLAN-ID>	Specifies a single VLAN or a range of VLANs as the match criteria. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the VLANs identified here are permitted. • <VLAN-ID> – Specify the VLAN ID. A range of VLANs is represented by the start and end VLAN IDs separated by a hyphen (for example, 12-20). Use this option with WLANs and port ACLs.
host <SOURCE-HOST-IP>	Identifies a specific host (as the source to match) by its IP address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the specified host are permitted. • <SOURCE-HOST-IP> – Specify the source host's exact IP address in the A.B.C.D format.
<DEST-IP/MASK>	Specifies the destination IP address and mask (A.B.C.D/M) to match. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to the specified destinations are permitted.
any	Specifies the destination as any destination IP address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to any destination are permitted.
host <DEST-HOST-IP>	Identifies a specific host (as the destination to match) by its IP address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addresses to the specified host are permitted. • <SOURCE-HOST-IP> – Specify the destination host's exact IP address in the A.B.C.D format.
<NETWORK-GROUP-ALIAS -NAME>	Applies a network-group alias to identify the destination IP addresses. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to the destinations identified in the network-group alias are permitted. • <NETWORK-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured). After specifying the source and destination IP address(es), specify the action taken in case of a match.
log	Logs all deny events matching this entry. If a source and/or destination IP address is matched (i.e. a packet (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) is received from a specified IP address and/or is destined for a specified IP address), an event is logged.
rule-precedence <1-5000> rule-description <LINE>	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Assigns a precedence for this permit rule • <1-5000> – Specify a value from 1 - 5000. Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • rule-description – Optional. Configures a description for this permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

```
permit [tcp|udp] [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan
<VLAN-ID>|host <SOURCE-HOST-IP>]
[<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|eq <SOURCE-PORT>|host
<DEST-HOST-IP>|range <START-PORT> <END-PORT>] [eq [<1-65535>|<SERVICE-NAME>|
bgp|dns|ftp|ftp-data|gopher|https|ldap|nntp|ntp|pop3|sip|smtp|ssh|telnet|tftp
|www]|
range <START-PORT> <END-PORT>] (log,rule-precedence <1-5000>)
{(rule-description <LINE>)}
```

tcp	Applies this permit rule to TCP packets only
udp	Applies this deny rule to UDP packets only
<SOURCE-IP/MASK>	This keyword is common to the 'tcp' and 'udp' parameters. Specifies the source IP address and mask (A.B.C.D/M) to match. TCP/UDP packets received from the specified sources are permitted.
<NETWORK-GROUP-ALIAS-NAME>	This keyword is common to the 'tcp' and 'udp' parameters. Applies a network-group alias to identify the source IP addresses. TCP/UDP packets received from the VLANs identified here are permitted. • <NETWORK-ALIAS-GROUP-NAME> – Specify the network-group alias name (should be existing and configured). After specifying the source and destination IP address(es), specify the action taken in case of a match.
any	This keyword is common to the 'tcp' and 'udp' parameters. Specifies the source as any source IP address. TCP/UDP packets received from any source are permitted.
from-vlan <VLAN-ID>	This keyword is common to the 'tcp' and 'udp' parameters. Specifies a single VLAN or a range of VLANs as the match criteria. TCP/UDP packets received from the VLANs identified here are permitted. • <VLAN-ID> – Specify the VLAN ID. To configure a range of VLANs, enter the start and end VLAN IDs separated by a hyphen (for example, 12-20). Use this option with WLANs and port ACLs.
host <SOURCE-HOST-IP>	Identifies a specific host (as the source to match) by its IP address. TCP/UDP packets received from the specified host are permitted. • <SOURCE-HOST-IP> – Specify the source host's exact IP address in the A.B.C.D format.
<DEST-IP/MASK>	This keyword is common to the 'tcp' and 'udp' parameters. Sets the destination IP address and mask (A.B.C.D/M) to match. TCP/UDP packets addressed to the specified destinations are permitted.
any	This keyword is common to the 'tcp' and 'udp' parameters. Specifies the destination as any destination IP address. TCP/UDP packets received from any destination are permitted.
eq <SOURCE-PORT>	Identifies a specific source port • <SOURCE-PORT> – Specify the exact source port.
host <DEST-HOST-IP>	Identifies a specific host (as the destination to match) by its IP address. TCP/UDP packets addressed to the specified host are permitted. • <DEST-HOST-IP> – Specify the destination host's exact IP address in the A.B.C.D format.
<NETWORK-GROUP-ALIAS-NAME>	This keyword is common to the 'tcp' and 'udp' parameters. Applies a network-group alias to identify the destination IP addresses. TCP/UDP packets destined to the addresses identified in the network-group alias are permitted. • <NETWORK-ALIAS-GROUP-NAME> – Specify the network-group alias name (should be existing and configured).
range <START-PORT> <END-PORT>	Specifies a range of source ports • <START-PORT> – Specify the first port in the range. • <END-PORT> – Specify the last port in the range.

eq [<1-65535>| <SERVICE-NAME>| |bgp|dns|ftp| ftp-data|gopher| https|ldap|nntp|ntp| pop3|sip|smtp| ssh|telnet| tftp|www]	Identifies a specific destination or protocol port to match • <1-65535> – The destination port is designated by its number • <SERVICE-NAME> – Specifies the service name • bgp – The designated *Border Gateway Protocol* (BGP) protocol port (179) • dns – The designated *Domain Name System* (DNS) protocol port (53) • ftp – The designated *File Transfer Protocol* (FTP) protocol port (21) • ftp-data – The designated FTP data port (20) • gropher – The designated GROPHER protocol port (70) • https – The designated HTTPS protocol port (443) • ldap – The designated *Lightweight Directory Access Protocol* (LDAP) protocol port (389) • nntp – The designated *Network News Transfer Protocol* (NNTP) protocol port (119) • ntp – The designated *Network Time Protocol* (NTP) protocol port (123) • pop3 – The designated POP3 protocol port (110) • sip – The designated *Session Initiation Protocol* (SIP) protocol port (5060) • smtp – The designated *Simple Mail Transfer Protocol* (SMTP) protocol port (25) • ssh – The designated *Secure Shell* (SSH) protocol port (22) • telnet – The designated Telnet protocol port (23) • tftp – The designated *Trivial File Transfer Protocol* (TFTP) protocol port (69) • www – The designated www protocol port (80)
range <START-PORT> <END-PORT>	Specifies a range of destination ports • <START-PORT> – Specify the first port in the range. • <END-PORT> – Specify the last port in the range.
log	Logs all permit events matching this entry. If a source and/or destination IP address or port is matched (i.e. a TCP/UDP packet is received from a specified IP address and/or is destined for a specified IP address), an event is logged.
rule-precedence <1-5000> rule-description <LINE>	The following keywords are recursive and common to all of the above: • rule-precedence – Assigns a precedence for this permit rule • <1-5000> – Specify a value from 1 - 5000. Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • rule-description – Optional. Configures a description for this permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

Usage Guidelines:

Use this command to permit traffic between networks/hosts based on the protocol type selected in the access list. The following protocols are supported:

- IP
- ICMP
- ICP
- UDP
- PROTO (any Internet protocol other than TCP, UDP, and ICMP)

The last ACE in the access list is an implicit deny statement.

Whenever the interface receives the packet, its content is checked against all the ACEs in the ACL. The packet is allowed or denied based on the ACL configuration.

- Filtering on TCP or UDP allows you to specify port numbers as filtering criteria.
- Select ICMP to allow/deny packets. Selecting ICMP filters ICMP packets based on ICMP type and code.

NOTE
The log option is functional only for router ACL's. The log option displays an informational logging message about the packet matching the entry sent to the console.

Example

```
rfs7000-37FABE(config-ip-acl-test)#show context
ip access-list test
rfs7000-37FABE(config-ip-acl-test)#

rfs7000-37FABE(config-ip-acl-test)#permit ip 172.16.10.0/24 any log
rule-precedence 750
rfs7000-37FABE(config-ip-acl-test)#permit tcp 172.16.10.0/24 any log
rule-precedence 800

rfs7000-37FABE(config-ip-acl-test)#show context
ip access-list test
 permit ip 172.16.10.0/24 any log rule-precedence 750
 permit tcp 172.16.10.0/24 any log rule-precedence 800
rfs7000-37FABE(config-ip-acl-test)#
```

Related Commands:

no	Removes a specified IP permit access rule
alias	Creates and configures aliases (network, VLAN, and service)

mac-access-list

ACCESS-LIST

The following table summarizes MAC Access list configuration commands.

Command	Description	Reference
deny	Creates a new deny access rule or modifies an existing rule. A deny access rule marks packets for rejection.	page 917
disable	Disables a MAC deny or permit rule without removing it from the ACL	page 919
insert	Inserts a rule in an MAC ACL without overwriting or replacing an exciting rule having the same precedence	page 921
no	Removes a deny and/or a permit access rule from a MAC ACL	page 923
permit	Creates a new permit access rule or modifies an existing rule. A deny access rule marks packets for forwarding.	page 925
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 394

Command	Description	Reference
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

deny

mac-access-list

Creates a deny rule that marks packets (from a specified source MAC and/or to a specified destination MAC) for rejection. You can also use this command to modify an existing deny rule.

NOTE
Use a decimal value representation to implement a `permit/deny` designation for a packet. The command set for MAC ACLs provide the hexadecimal values for each listed EtherType. Use the decimal equivalent of the EtherType listed for any other EtherType.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
deny [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host <SOURCE-HOST-MAC>]
          [<DESTINATION-MAC> <DESTINATION-MAC-MASK>|any|host <DEST-HOST-MAC>]
          (dot1p <0-7>,type
[8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp],
          vlan <1-4095>,log,rule-precedence <1-5000>) {(rule-description
<LINE>)}
```

Parameters

```
deny [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host <SOURCE-HOST-MAC>]
[<DESTINATION-MAC> <DESTINATION-MAC-MASK>|any|host <DEST-HOST-MAC>]
(dot1p <0-7>,type
[8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp],
vlan <1-4095>,log,rule-precedence <1-5000>) {(rule-description <LINE>)}
```

<SOURCE-MAC> <SOURCE-MAC-MASK>	Configures the source MAC address and mask to match • <SOURCE-MAC> – Specify the source MAC address to match. • <SOURCE-MAC-MASK> – Specify the source MAC address mask. Packets received from the specified MAC addresses are dropped.
any	Identifies all devices as the source to deny access. Packets received from any source are dropped.
host <SOURCE-HOST-MAC>	Identifies a specific host as the source to deny access • <SOURCE-HOST-MAC> – Specify the source host's exact MAC address to match. Packets received from the specified host are dropped.

<DEST-MAC> <DEST-MAC-MASK>	Configures the destination MAC address and mask to match • <DEST-MAC> – Specify the destination MAC address to match. • <DEST-MAC-MASK> – Specify the destination MAC address mask to match. Packets addressed to the specified MAC addresses are dropped.
any	Identifies all devices as the destination to deny access. Packets addressed to any destination are dropped.
host <DEST-HOST-MAC>	Identifies a specific host as the destination to deny access • <DEST-HOST-MAC> – Specify the destination host's exact MAC address to match. Packets addressed to the specified host are dropped.
dotp1p <0-7>	Configures the 802.1p priority value. Sets the service classes for traffic handling • <0-7> – Specify 802.1p priority from 0 - 7.
type [8021q|<1-65535>| aarp|appletalk| arp|ip|ipv6|ipx|mint| rarp|wisp]	Configures the EtherType value An EtherType is a two-octet field in an Ethernet frame that indicates the protocol encapsulated in the payload of the frame. The EtherType values are: • 8021q – Indicates a 802.1q payload (0x8100) • <1-65535> – Indicates the EtherType protocol number • aarp – Indicates the Appletalk *Address Resolution Protocol* (ARP) payload (0x80F3) • appletalk – Indicates the Appletalk Protocol payload (0x809B) • arp – Indicates the ARP payload (0x0806) • ip – Indicates the Internet Protocol, Version 4 (IPv4) payload (0x0800) • ipv6 – Indicates the Internet Protocol, Version 6 (IPv6) payload (0x86DD) • ipx – Indicates the Novell's IPX payload (0x8137) • mint – Indicates the MiNT protocol payload (0x8783) • rarp – Indicates the reverse *Address Resolution Protocol* (ARP) payload (0x8035) • wisp – Indicates the *Wireless Internet Service Provider* (WISP) payload (0x8783)
vlan <1-4095>	Configures the VLAN where the traffic is received • <1-4095> – Specify the VLAN ID from 1 - 4095.
log	Logs all deny events matching this entry. If a source and/or destination MAC address is matched (i.e. a packet is received from a specified MAC address or is destined for a specified MAC address), an event is logged.
rule-precedence <1-5000> rule-description <LINE>	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Assigns a precedence for this deny rule • <1-5000> – Specify a value from 1 - 5000. Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • rule-description – Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

Usage Guidelines:

The deny command disallows traffic based on layer 2 (data-link layer) data. The MAC access list denies traffic from a particular source MAC address or any MAC address. It can also disallow traffic from a list of MAC addresses based on the source mask.

The MAC access list can disallow traffic based on the VLAN and EtherType.

- ARP
- WISP
- IP
- 802.1q

NOTE
MAC ACLs always takes precedence over IP based ACLs.

The last ACE in the access list is an implicit deny statement. Whenever the interface receives the packet, its content is checked against all the ACEs in the ACL. It is allowed or denied based on the ACL's configuration.

Example

```
rfs4000-229D58(config-mac-acl-test)#deny 41-85-45-89-66-77 ff-ff-ff-00-00-00
any
 vlan 1 rule-precedence 1
rfs4000-229D58(config-mac-acl-test)#

rfs4000-229D58(config-mac-acl-test)#deny host 00-01-ae-00-22-11 any
rule-precedence 2
rfs4000-229D58(config-mac-acl-test)#

rfs4000-229D58(config-mac-acl-test)#show context
mac access-list test
 deny 41-85-45-89-66-77 FF-FF-FF-00-00-00 any vlan 1 rule-precedence 1
 deny host 00-01-AE-00-22-11 any rule-precedence 2
rfs4000-229D58(config-mac-acl-test)#
```

The MAC ACL (in the example below) denies traffic from any source MAC address to a particular host MAC address:

```
rfs7000-37FABE(config-mac-acl-test)#deny any host 00:01:ae:00:22:11
rfs7000-37FABE(config-mac-acl-test)#
```

The following example denies traffic between two hosts based on MAC addresses:

```
rfs7000-37FABE(config-mac-acl-test)#deny host 01:02:fe:45:76:89 host
01:02:89:78:78:45
rfs7000-37FABE(config-mac-acl-test)#
```

Related Commands:

no	Removes a specified MAC deny access rule

disable

mac-access-list

Disables a MAC deny or permit rule without removing it from the ACL. A disabled rule is inactive and is not used to filter packets.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
disable [deny|permit] [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host
<SOURCE-HOST-MAC>]
          [<DEST-MAC> <DEST-MAC-MASK>|any|host <DEST-HOST-MAC>] (dot1p
<0-7>,type [8021q|
          <1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp],vlan
<1-4095>) log
          (rule-recedence <1-5000>) {(rule-description <LINE>)}
```

Parameters

```
disable [deny|permit] [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host
<SOURCE-HOST-MAC>]
[<DEST-MAC> <DEST-MAC-MASK>|any|host <DEST-HOST-MAC>] (dot1p <0-7>,type
[8021q|
<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp],vlan <1-4095>) log
(rule-recedence <1-5000>) {(rule-description <LINE>)}
```

disable [deny|permit]	Disables a deny or permit access rule without removing it from the MAC ACL Provide the exact values used to configure the deny or permit rule that is to be disabled.
<SOURCE-MAC> <SOURCE-MAC-MASK>	Specifies the source MAC address and mask to match • <SOURCE-MAC> – Specify the source MAC address to match. • <SOURCE-MAC-MASK> – Specify the source MAC address mask.
any	Select ‘any’ if the rule is applicable to any source MAC address
host <SOURCE-HOST-MAC>	Specify the source host’s exact MAC address
<DEST-MAC> <DEST-MAC-MASK>	Specifies the destination MAC address and mask to match • <DEST-MAC> – Specify the destination MAC address. • <DEST-MAC-MASK> – Specify the destination MAC address mask.
any	Select ‘any’ if the rule is applicable to any destination MAC address
host <DEST-HOST-MAC>	Specify the destination host’s exact MAC address
log	The following keyword defines the action taken when a packet matches any or all of the above specified criteria • log – Logs a record. when a packet matches the specified criteria
dotp1p <0-7>	Specify the 802.1p priority from 0 - 7.
type [8021q|<1-65535>| aarp|appletalk| arp|ip|ipv6|ipx|mint| rarp|wisp]	Use the available options to specify the EtherType value.
vlan <1-4095>	Specify the VLAN ID(s)
log	Select log, if the rule has been configured to log records in case of a match.
rule-precedence <1-5000> {(rule-description <LINE>)}	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Provide the precedence assigned to this deny or permit rule. • <1-5000> – Specify a value from 1 - 5000. The rule with the specified precedence is removed form the MAC ACL. • rule-description <LINE> – Optional. Enter the description configured for this deny or permit rule.

Example

```
The following example shows the MAC access list ‘test’ settings before the
‘disable’ command is executed:
```

```
rfs4000-229D58(config-mac-acl-test)#show context
mac access-list test
 deny 41-85-45-89-66-77 FF-FF-FF-00-00-00 any vlan 1 rule-precedence 1
 deny host 00-01-AE-00-22-11 any rule-precedence 2
rfs4000-229D58(config-mac-acl-test)#

rfs4000-229D58(config-mac-acl-test)#disable deny host 00-01-AE-00-22-11 any
rule-precedence 2

The following example shows the MAC access list ‘test’ settings after the
‘disable’ command is executed:

rfs4000-229D58(config-mac-acl-test)#show context
mac access-list test
 deny 41-85-45-89-66-77 FF-FF-FF-00-00-00 any vlan 1 rule-precedence 1
 disable deny host 00-01-AE-00-22-11 any rule-precedence 2
rfs4000-229D58(config-mac-acl-test)#
```

Related Commands:

no	Enables a disabled deny or permit rule
deny	Creates a new deny access rule or modifies an existing rule
permit	Creates a new permit access rule or modifies an existing rule

insert

mac-access-list

Enables the insertion of a rule in an MAC ACL without overwriting or replacing an existing rule having the same precedence

The insert option allows a new rule to be inserted within a MAC ACL. Consider an MAC ACL consisting of rules having precedences 1, 2, 3, 4, 5, and 6. You want to insert a new rule with precedence 4, without overwriting the existing precedence 4 rule. Using the insert option inserts the new rule prior to the existing one. The existing precedence 4 rule’s precedence changes to 5, and the change cascades down the list of rules within the ACL. That means rule 5 becomes rule 6, and rule 6 becomes rule 7.

NOTE
NOT using *insert* when creating a new rule having the same precedence as an existing rule, overwrites the existing rule.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
insert [deny|permit] <PARAMETERS> (dot1p <0-7>,type
[8021q|<1-65535>|aarp|appletalk|
          arp|ip|ipv6|ipx|mint|rarp|wisp],vlan <1-4095>,log,rule-precedence
<1-5000>)
          {(rule-description <LINE>)}
```

Parameters

```
insert [deny|permit] <PARAMETERS> (log,mark [8021p <0-7>|dscp <0-63>],
rule-precedence <1-5000>) {(rule-description <LINE>)}
```

insert [deny|permit]	Inserts a deny or permit rule within an MAC ACL
<PARMETERS>	Provide the match criteria for this deny/permit rule. Packets will be filtered based on the criteria set here. For more information on the deny rule, see *deny*. For more information on the permit rule, see *permit*.
dotp1p <0-7>	Configures the 802.1p priority value. Sets the service classes for traffic handling • <0-7> – Specify 802.1p priority from 0 - 7.
type [8021q|<1-65535>| aarp|appletalk| arp|ip|ipv6|ipx|mint| rarp|wisp]	Configures the EtherType value An EtherType is a two-octet field in an Ethernet frame that indicates the protocol encapsulated in the payload of the frame. The EtherType values are: • 8021q – Indicates a 802.1q payload (0x8100) • <1-65535> – Indicates the EtherType protocol number • aarp – Indicates the Appletalk ARP payload (0x80F3) • appletalk – Indicates the Appletalk Protocol payload (0x809B) • arp – Indicates the ARP payload (0x0806) • ip – Indicates the IPv4 payload (0x0800) • ipv6 – Indicates the IPv6 payload (0x86DD) • ipx – Indicates the Novell's IPX payload (0x8137) • mint – Indicates the MiNT protocol payload (0x8783) • rarp – Indicates the reverse ARP payload (0x8035) • wisp – Indicates the WISP payload (0x8783)
vlan <1-4095>	Configures the VLAN where the traffic is received • <1-4095> – Specify the VLAN ID from 1 - 4095.
log	Logs all deny/permit events matching this entry. If a source and/or destination MAC address is matched (i.e. a packet is received from a specified MAC address or is destined for a specified MAC address), an event is logged.
rule-precedence <1-5000> rule-description <LINE>	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Assigns a precedence for this deny rule • <1-5000> – Specify a value from 1 - 5000. Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • rule-description – Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

Example

```
rfs4000-229D58(config-mac-acl-test1)#deny 11-22-33-44-55-66 11-22-33-44-55-77
any rule-precedence 1

rfs4000-229D58(config-mac-acl-test1)#deny host B4-C7-99-6D-CD-9B any
rule-precedence 2

rfs4000-229D58(config-mac-acl-test1)#show context
mac access-list test1
 deny 11-22-33-44-55-66 11-22-33-44-55-77 any rule-precedence 1
```

```
 deny host B4-C7-99-6D-CD-9B any rule-precedence 2
rfs4000-229D58(config-mac-acl-test1)#

In the following example a new rule is inserted between the rules having
precedences 1 and 2. The precedence of the existing precedence ‘2’ rule
changes to precedence 3.

rfs4000-229D58(config-mac-acl-test1)#insert permit host B4-C7-99-6D-B5-D6 host
B4-C7-99-6D-CD-9B rule-precedence 2

rfs4000-229D58(config-mac-acl-test1)#show context
mac access-list test1
 deny 11-22-33-44-55-66 11-22-33-44-55-77 any rule-precedence 1
 permit host B4-C7-99-6D-B5-D6 host B4-C7-99-6D-CD-9B rule-precedence 2
 deny host B4-C7-99-6D-CD-9B any rule-precedence 3
rfs4000-229D58(config-mac-acl-test1)#
```

no

mac-access-list

Negates a command or sets its default

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no [deny|disable|permit]

no [deny|permit] [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host <SOURCE-HOST-MAC>]
          [<DEST-MAC> <DEST-MAC-MASK>|any|host <DEST-HOST-MAC>]
          (dot1p <0-7>,type
[8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|
          wisp],vlan <1-4095>) log (rule-precedence <1-5000>)
{(rule-description <LINE>)}

no disable [deny|permit] <RULE-PARAMETERS>
```

Parameters

```
no [deny|permit] [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host <SOURCE-HOST-MAC>]
[<DEST-MAC> <DEST-MAC-MASK>|any|host <DEST-HOST-MAC>] (dot1p <0-7>,
type [8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp],vlan
<1-4095>) log (rule-precedence <1-5000>) {(rule-description <LINE>)}
```

no [deny|permit]	Removes a deny or permit rule from the MAC ACL
<SOURCE-MAC> <SOURCE-MAC-MASK>	Specify the source MAC address and mask
any	Select ‘any’ if the rule is applicable to any source MAC address

host <SOURCE-HOST-MAC>	Specify the source host's exact MAC address.
<DEST-MAC> <DEST-MAC-MASK>	Specify the destination MAC address and mask
any	Identifies all devices as the destination to deny/permit access
host <DEST-HOST-MAC>	Specify the destination host's exact MAC address.
dotp1p <0-7>	Specify the 802.1p priority value from 0 -7.
type [8021q|<1-65535>| aarp|appletalk|arp|ip|ipv6| ipx|mint|rarp|wisp]	Specify the EtherType value.
vlan <1-4095>	Specify the VLAN ID.
log	Select log, if the rule has been configured to log records in case of a match.
mark [8021p <0-7>| dscp <0-63>]	This is specific to the MAC ACL permit rule. Marks packets that match the ACL rule • 8021p <0-7> – Modifies 802.1p VLAN user priority from 0 - 7 • dscp <0-63> – Modifies DSCP TOS bits in the IP header from 0 - 63
rule-precedence <1-5000>	Specify the rule precedence. The rule with the specified rule precedence is removed from the MAC ACL.
rule-description <LINE>	Optional. Provide the description configured for the rule.

```
no disable [deny|permit] <RULE-PARAMETERS>
```

no disabled [deny|permit]	Removes a disabled deny or permit rule from the selected IP access list
<RULE-PARAMETERS>	Enter the exact parameters used when configuring the rule.
rule-precedence <1-5000> rule-description <LINE>}	Specify the precedence assigned to this disabled deny/permit rule. • rule-description – Optional. Specify the rule description. The system removes the disabled rule from the selected ACL.

Example

```
rfs7000-37FABE(config-mac-acl-test)#show context
mac access-list test
 permit host 11-22-33-44-55-66 any log mark 8021p 3 rule-precedence 600
 permit host 22-33-44-55-66-77 host 11-22-33-44-55-66 type ip log
rule-precedence 610
deny any host 33-44-55-66-77-88 log rule-precedence 700

rfs7000-37FABE(config-mac-acl-test)#no deny any host 33-44-55-66-77-88 log
rule-precedence 700

rfs7000-37FABE(config-mac-acl-test)#show context
mac access-list test
 permit host 11-22-33-44-55-66 any log mark 8021p 3 rule-precedence 600
 permit host 22-33-44-55-66-77 host 11-22-33-44-55-66 type ip log
rule-precedence 610
```

Related Commands:

deny	Creates a MAC deny ACL
permit	Creates a MAC permit ACL

permit

mac-access-list

Creates a permit rule that marks packets (from a specified source MAC and/or to a specified destination MAC) for forwarding. You can also use this command to modify an existing permit rule.

NOTE
Use a decimal value representation to implement a `permit/deny` designation for a packet. The command set for MAC ACLs provide the hexadecimal values for each listed EtherType. Use the decimal equivalent of the EtherType listed for any other EtherType.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
permit [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host <SOURCE-HOST-MAC>]
          [<DESTINATION-MAC> <DESTINATION-MAC-MASK>|any|host <DEST-HOST-MAC>]
          (dot1p <0-7>,type
[8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|
          wisp],vlan <1-4095>) log (rule-precedence <1-5000>)
{(rule-description <LINE>)}
```

Parameters

```
permit [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host <SOURCE-HOST-MAC>]
[<DEST-MAC> <DEST-MAC-MASK>|any|host <DEST-HOST-MAC>]
(dot1p <0-7>,type
[8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp],
vlan <1-4095>) log (rule-precedence <1-5000>) {(rule-description <LINE>)}
```

<SOURCE-MAC> <SOURCE-MAC-MASK>	Configures the source MAC address and mask to match • <SOURCE-MAC> – Specify the source MAC address to match. • <SOURCE-MAC-MASK> – Specify the source MAC address mask. Packets addressed to the specified MAC addresses are forwarded.
any	Identifies all devices as the source to permit access. Packets addressed from any source are forwarded.
host <SOURCE-HOST-MAC>	Identifies a specific host as the source to permit access • <SOURCE-HOST-MAC> – Specify the source host's exact MAC address to match. Packets addressed to the specified host are forwarded.

<DEST-MAC> <DEST-MAC-MASK>	Configures the destination MAC address and mask to match • <DEST-MAC> – Specify the destination MAC address to match. • <DEST-MAC-MASK> – Specify the destination MAC address mask to match. Packets addressed to the specified MAC addresses are forwarded.
DEST-MAC-MASK	Specifies the destination MAC address mask to match
any	Identifies all devices as the destination to permit access. Packets addressed to any destination are forwarded.
host <DEST-HOST-MAC>	Identifies a specific host as the destination to permit access • <DEST-HOST-MAC> – Specify the destination host's exact MAC address to match. Packets addressed to the specified host are forwarded.
dotp1p <0-7>	Configures the 802.1p priority value. Sets the service classes for traffic handling • <0-7> – Specify 802.1p priority from 0 - 7.
type [8021q|<1-65535>| aarp|appletalk| arp|ip|ipv6|ipx|mint| rarp|wisp]	Configures the EtherType value An EtherType is a two-octet field in an Ethernet frame that indicates the protocol encapsulated in the payload of the frame. The EtherType values are: • 8021q – Indicates a 802.1q payload (0x8100) • <1-65535> – Indicates the EtherType protocol number • aarp – Indicates the Appletalk *Address Resolution Protocol* (ARP) payload (0x80F3) • appletalk – Indicates the Appletalk Protocol payload (0x809B) • arp – Indicates the ARP payload (0x0806) • ip – Indicates the Internet Protocol, Version 4 (IPv4) payload (0x0800) • ipv6 – Indicates the Internet Protocol, Version 6 (IPv6) payload (0x86DD) • ipx – Indicates the Novell's IPX payload (0x8137) • mint – Indicates the MiNT protocol payload (0x8783) • rarp – Indicates the reverse *Address Resolution Protocol* (ARP) payload (0x8035) • wisp – Indicates the *Wireless Internet Service Provider* (WISP) payload (0x8783)
vlan <1-4095>	Configures the VLAN ID • <1-4095> – Specify the VLAN ID from 1 - 4095.
log	Logs all permit events matching this entry. If a source and/or destination MAC address is matched (i.e. a packet is addressed to a specified MAC address or is destined for a specified MAC address), an event is logged.
rule-precedence <1-5000> rule-description <LINE>	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Assigns a precedence for this permit rule • <1-5000> – Specify a value from 1 - 5000. Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • rule-description – Optional. Configures a description for this permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

Usage Guidelines:

The permit command in the MAC ACL allows traffic based on layer 2 (data-link layer) information. A MAC access list permits traffic from a source MAC address or any MAC address. It also has an option to allow traffic from a list of MAC addresses (based on the source mask).

The MAC access list can be configured to allow traffic based on VLAN information, or Ethernet type. Common types include:

- ARP
- WISP
- IP
- 802.1q

Layer 2 traffic is not allowed by default. To adopt an access point through an interface, configure an ACL to allow an Ethernet WISP.

Use the mark option to specify the type of service (tos) and priority value. The tos value is marked in the IP header and the 802.1p priority value is marked in the dot1q frame.

Whenever the interface receives the packet, its content is checked against all the ACEs in the ACL. It is marked based on the ACL's configuration.

NOTE
To apply an IP based ACL to an interface, a MAC access list entry is mandatory to allow ARP. A MAC ACL always takes precedence over IP based ACLs.

Example

```
rfs7000-37FABE(config-mac-acl-test)#permit host 11-22-33-44-55-66 any log mark
8021p 3 rule-precedence 600

rfs7000-37FABE(config-mac-acl-test)#permit host 22-33-44-55-66-77 host
11-22-33-44-55-66 type ip log rule-precedence 610

rfs7000-37FABE(config-mac-acl-test)#show context
mac access-list testPF
 permit host 11-22-33-44-55-66 any log mark 8021p 3 rule-precedence 600
 permit host 22-33-44-55-66-77 host 11-22-33-44-55-66 type ip log
rule-precedence 610
rfs7000-37FABE(config-mac-acl-test)#
```

Related Commands:

no	Removes or resets a specified MAC ACL permit rule

Chapter

DHCP-SERVER-POLICY 13

This chapter summarizes *Dynamic Host Control Protocol* (DHCP) server policy commands in the CLI command structure.

DHCP automatically assigns network IP addresses to requesting clients to enable them access to network resources. DHCP tracks IP address assignments, their lease times and their availability. Each subnet can be configured with its own address pool. Whenever a DHCP client requests an IP address, the DHCP server assigns an IP address from that subnet's address pool. When the controller's (wireless controller, service platform, or access point) onboard DHCP server allocates an address to a DHCP client, the client is assigned a lease, which expires after a pre-determined interval. Before a lease expires, wireless clients (with assigned leases) are expected to renew them to continue using the addresses. Once the lease expires, the client is no longer permitted to use the leased IP address. The controller's DHCP server policy ensures all IP addresses are unique, and no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). IP address management is conducted by a controller's DHCP server and not by an administrator.

The controller's internal DHCP server groups wireless clients based on defined user-class options. Clients with a defined set of user-class values are segregated by class. A DHCP server can associate multiple classes to each pool. Each class in a pool is assigned an exclusive range of IP addresses. DHCP clients are compared against classes. If the client matches one of the classes assigned to the pool, it receives an IP address from the range assigned to the class. If the client doesn't match any of the classes in the pool, it receives an IP address from a default pool range (if defined). Multiple IP addresses for a single VLAN allow the configuration of multiple IP addresses, each belonging to different subnets. Class configuration allows a DHCP client to obtain an address from the first pool to which the class is assigned.

Use the (config) instance to configure DHCP server policy parameters. To navigate to the config DHCP server policy instance, use the following commands:

```
<DEVICE>(config)#dhcp-server-policy <POLICY-NAME>

rfs7000-37FABE(config)#dhcp-server-policy test
rfs7000-37FABE(config-dhcp-server-policy-test)#

rfs7000-37FABE(config-dhcp-policy-test)#?
DHCP policy Mode commands:
  bootp       BOOTP specific configuration
  dhcp-class  Configure DHCP class (for address allocation using DHCP
              user-class options)
  dhcp-pool   Configure DHCP server address pool
  no          Negate a command or set its defaults
  option      Define DHCP server option
  ping        Specify ping parameters used by DHCP Server

  clrscr      Clears the display screen
  commit      Commit all changes made in this session
  do          Run commands from Exec mode
  end         End current mode and change to EXEC mode
  exit        End current mode and down to previous mode
```

```
  help        Description of the interactive help system
  revert      Revert changes
  service     Service Commands
  show        Show running system information
  write       Write running configuration to memory or terminal

rfs7000-37FABE(config-dhcp-policy-test)#
```

dhcp-server-policy

Table 11 summarizes DHCP server policy configuration commands.

TABLE 11 DHCP-Server-Policy-Config Commands

Command	Description	Reference
bootp	Configures a BOOTP specific configuration	page 930
dhcp-class	Configures a DHCP server class	page 931
dhcp-pool	Configures a DHCP server address pool	page 935
no	Negates a command or sets its default	page 973
option	Defines the DHCP option used in DHCP pools	page 975
ping	Specifies ping parameters used by a DHCP server	page 976
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

bootp

dhcp-server-policy

Configures a BOOTP specific configuration

Bootstrap Protocol (BOOTP) requests are used by UNIX diskless workstations to obtain the location of their boot image and IP address within the managed network. A BOOTP configuration server provides this information and also assigns an IP address from a configured pool of IP addresses. By default, all BOOTP requests are forwarded to the BOOTP configuration server by the controller. When enabled, this feature allows controllers, using this DHCP server policy, to ignore BOOTP requests.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
bootp ignore
```

Parameters

```
bootp ignore
```

bootp ignore	Enables controllers to ignore BOOTP requests

Example

```
rfs7000-37FABE(config-dhcp-policy-test)#bootp ignore

rfs7000-37FABE(config-dhcp-policy-test)#show context
dhcp-server-policy test
 bootp ignore
rfs7000-37FABE(config-dhcp-policy-test)#
```

Related Commands:

no	Disables the ignore BOOTP requests option

dhcp-class

dhcp-server-policy

A DHCP user class applies different DHCP settings to a set of wireless clients. Wireless clients using the same DHCP settings are grouped under one DHCP class. Grouping users into classes facilitates the provision of differentiated service.

The following table summarizes DHCP class configuration commands.

Command	Description	Reference
dhcp-class	Creates a DHCP class and enters its configuration mode	page 931
dhcp-class-mode commands	Invokes DHCP class configuration commands	page 932

dhcp-class

dhcp-class

Creates a DHCP server class and enters its configuration mode. Use this command to configure user class option values. Once defined, the controller's internal DHCP server uses the configured values to group wireless clients into DHCP classes. Therefore, each user class consists of wireless clients sharing the same set of user class values.

You can also use this command to modify an existing DHCP user class settings.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
dhcp-class <DHCP-CLASS-NAME>
```

Parameters

```
dhcp-class <DHCP-CLASS-NAME>
```

<DHCP-CLASS-NAME>	Creates a DHCP user class • <DHCP-CLASS-NAME> – Specify a name that appropriately identifies this class of wireless clients. If the class does not exist, it is created. The class name should not exceed 32 characters in length.

Example

```
rfs7000-37FABE(config-dhcp-policy-test)#dhcp-class dhcpclass1

rfs7000-37FABE(config-dhcp-policy-test-class-dhcpclass1)#?
DHCP class Mode commands:
  multiple-user-class  Enable multiple user class option
  no                   Negate a command or set its defaults
  option               Configure DHCP Server options

  clrscr               Clears the display screen
  commit               Commit all changes made in this session
  do                   Run commands from Exec mode
  end                  End current mode and change to EXEC mode
  exit                 End current mode and down to previous mode
  help                 Description of the interactive help system
  revert               Revert changes
  service              Service Commands
  show                 Show running system information
  write                Write running configuration to memory or terminal

rfs7000-37FABE(config-dhcp-policy-test-class-dhcpclass1)#
```

Related Commands:

no	Removes a configured DHCP user class policy

dhcp-class-mode commands

dhcp-class

Use DHCP class mode commands to configure the parameters of the DHCP user class.

The following table summarizes DHCP user class configuration commands.

Command	Description	Reference
multiple-user-class	Enables or disables multiple user class option for this DHCP user class policy	page 933
no	Negates a command or sets its default	page 934
option	Configures DHCP user class options for this DHCP user class policy	page 935
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

multiple-user-class

dhcp-class-mode commands

Enables or disables multiple user class option for this DHCP user class policy. Enabling this option allows this user class to transmit multiple option values to other DHCP servers also supporting multiple user class options.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
multiple-user-class
```

Parameters

None

Example

```
rfs7000-37FABE(config-dhcp-policy-test-class-class1)#multiple-user-class

rfs7000-37FABE(config-dhcp-policy-test-class-dhcpclass1)#show context
 dhcp-class dhcpclass1
  multiple-user-class
rfs7000-37FABE(config-dhcp-policy-test-class-dhcpclass1)#
```

Related Commands:

no	Disables the multiple user class option for the selected DHCP user class policy

no

dhcp-class-mode commands

Removes this DHCP user class policy's settings

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no [multiple-user-class|option]
no option user-class <VALUE>
```

Parameters

```
no multiple-user-class
```

no multiple-user-class	Disables multiple user class options on this DHCP user class policy

```
no option user-class <VALUE>
```

no option user-class <VALUE>	Removes the DHCP user class option identified by the <VALUE> keyword

Example

```
The following example shows the DHCP class settings before the 'no' commands
are executed:

rfs7000-37FABE(config-dhcp-policy-test-class-dhcpclass1)#show context
 dhcp-class dhcpclass1
  option user-class hex
  multiple-user-class
rfs7000-37FABE(config-dhcp-policy-test-class-dhcpclass1)#

rfs7000-37FABE(config-dhcp-policy-test-class-class1)#no multiple-user-class
rfs7000-37FABE(config-dhcp-policy-test-class-dhcpclass1)#no option user-class
hex

The following example shows the DHCP class settings after the 'no' commands
are executed:

rfs7000-37FABE(config-dhcp-policy-test-class-dhcpclass1)#show context
 dhcp-class dhcpclass1
rfs7000-37FABE(config-dhcp-policy-test-class-dhcpclass1)#
```

Related Commands:

multiple-user-class	Enables or disables multiple user class option for this DHCP user class policy
option	Configures DHCP user class options for this DHCP user class policy

option

dhcp-class-mode commands

Configures DHCP user class options for this DHCP user class policy

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
option user-class <VALUE>
```

Parameters

```
option user-class <VALUE>
```

user-class <VALUE>	Configures DHCP user class options • <VALUE> – Specify the DHCP user class option's ASCII value.

Example

```
rfs7000-37FABE(config-dhcp-policy-test-class-class1)#option user-class hex

rfs7000-37FABE(config-dhcp-policy-test-class-dhcpclass1)#show context
 dhcp-class dhcpclass1
  option user-class hex
  multiple-user-class
rfs7000-37FABE(config-dhcp-policy-test-class-dhcpclass1)#
```

Related Commands:

no	Removes the configured DHCP user class option

dhcp-pool

dhcp-server-policy

The DHCP pool command creates and manages a pool of IP addresses. These IP addresses are assigned to devices using the DHCP protocol. IP addresses have to be unique for each device in the network. Since IP addresses are finite, DHCP ensures that every device, in the network, is issued a unique IP address by tracking the issue, release, and reissue of IP addresses.

The DHCP pool command configures a finite set of IP addresses that can be assigned whenever a device joins a network.

The following table summarizes DHCP pool configuration mode commands.

Command	Description	Reference
dhcp-pool	Creates a DHCP pool and enters its configuration mode	page 936
dhcp-pool-mode commands	Summarizes DHCP pool configuration mode commands	page 937

dhcp-pool

dhcp-pool

Configures a DHCP server address pool

DHCP services are available for specific IP interfaces. A pool (or range) of IP network addresses and DHCP options can be created for each IP interface defined. This range of addresses is available to DHCP enabled wireless devices on either a permanent or leased basis. This enables the reuse of limited IP address resources for deployment in any network. DHCP options are provided to each DHCP client with a DHCP response and provides DHCP clients information required to access network resources (default gateway, domain name, DNS server and WINS server configuration). An option exists to identify the vendor and functionality of a DHCP client. The information is a variable-length string of characters (or octets) with a meaning specified by the vendor of the DHCP client.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
dhcp-pool <POOL-NAME>
```

Parameters

```
dhcp-pool <POOL-NAME>
```

<POOL-NAME>	Creates a DHCP server address pool • <POOL-NAME> – Specify a name that appropriately identifies this DHCP address pool. If the pool does not exist, it is created. The pool name cannot be modified as part of the edit process. However, an obsolete address pool can be deleted.

Example

```
rfs7000-37FABE(config-dhcp-policy-test)#dhcp-pool pool1

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#?
DHCP pool Mode commands:
  address              Configure network pool's included addresses
  bootfile             Boot file name
  ddns                 Dynamic DNS Configuration
  default-router       Default routers
  dns-server           DNS Servers
  domain-name          Configure domain-name
```

```
  excluded-address     Prevent DHCP Server from assigning certain addresses
  lease                Address lease time
  netbios-name-server  NetBIOS (WINS) name servers
  netbios-node-type    NetBIOS node type
  network              Network on which DHCP server will be deployed
  next-server          Next server in boot process
  no                   Negate a command or set its defaults
  option               Raw DHCP options
  respond-via-unicast  Send DHCP offer and DHCP Ack as unicast messages
  static-binding       Configure static address bindings
  static-route         Add static routes to be installed on dhcp clients
  update               Control the usage of DDNS service

  clrscr               Clears the display screen
  commit               Commit all changes made in this session
  do                   Run commands from Exec mode
  end                  End current mode and change to EXEC mode
  exit                 End current mode and down to previous mode
  help                 Description of the interactive help system
  revert               Revert changes
  service              Service Commands
  show                 Show running system information
  write                Write running configuration to memory or terminal

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#
```

Related Commands:

no	Removes a specified DHCP address pool

dhcp-pool-mode commands

dhcp-pool

Configures the DHCP pool parameters

The following table summarizes DHCP pool configuration commands.

Command	Description	Reference
address	Specifies a range of addresses for a DHCP address pool	page 938
bootfile	Assigns a bootfile name. The bootfile name can contain letters, numbers, dots and hyphens. Consecutive dots and hyphens are not permitted.	page 939
ddns	Configures dynamic DNS parameters	page 940
default-router	Configures a default router or gateway IP address for the network pool	page 941
dns-server	Sets a DNS server's IP address available to all DHCP clients connected to the DHCP pool	page 942
domain-name	Sets the domain name for the network pool	page 943
excluded-address	Prevents a DHCP server from assigning certain addresses to the DHCP pool	page 944
lease	Sets a valid lease for the IP address used by DHCP clients in the DHCP pool	page 946
netbios-name-server	Configures a NetBIOS (WINS) name server's IP address	page 947
netbios-node-type	Defines the NetBIOS node type	page 948
network	Configures the network on which the DHCP server is deployed	page 949

Command	Description	Reference
next-server	Configures the next server in the boot process	page 950
no	Negates a command or sets its default	*no*
option	Configures RAW DHCP options	page 935
respond-via-unicast	Sends a DHCP offer and DHCP Ack as unicast messages	page 956
static-route	Configures a static route for a DHCP pool	page 956
update	Controls the usage of the DDNS service	page 957
static-binding	Configures static address bindings	page 958

address

dhcp-pool-mode commands

Adds IP addresses to the DHCP address pool. These IP addresses are assigned to each device joining the network.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
address [<IP>|<HOST-ALIAS-NAME>|range]

address [<IP>|<HOST-ALIAS-NAME>|range [<START-IP>|<START-HOST-ALIAS-NAME>]
[<END-IP>|
          <END-HOST-ALIAS-NAME>]] {class <DHCP-CLASS-NAME>}
```

Parameters

```
address [<IP>|<HOST-ALIAS-NAME>|range [<START-IP>|<START-HOST-ALIAS-NAME>]
[<END-IP>|
<END-HOST-ALIAS-NAME>]] {class <DHCP-CLASS-NAME>}
```

<IP>	Adds a single IP address to the DHCP address pool
<HOST-ALIAS-NAME>	Adds a single host mapped to the specified host alias. The host alias should be existing and configured. A network host alias maps a name to a single network host. For example, 'alias host $HOST 1.1.1.100'. In this example the host alias is '*$HOST*' and it maps to a single host '*1.1.1.100*'. For more information, see *alias*.

range [<START-IP>| <START-HOST-ALIAS-NAME>] [<END-IP>| <END-HOST-ALIAS-NAME>]	Adds a range of IP addresses to the DHCP address pool. Use one of the following options to provide the first IP address in the range: • <START-IP> – Specifies the first IP address in the range • <START-HOST-ALIAS-NAME> – Specifies a host alias, mapped to the first IP address in the range Use one of the following options to provide the last IP address in the range: • <END-IP> – Specifies the last IP address in the range • <END-HOST-ALIAS-NAME> – Specifies a host alias, mapped to the last IP address in the range The host aliases should be existing and configured.
class <DHCP-CLASS-NAME>	Optional. Applies additional DHCP options, or a modified set of options to those available to wireless clients. For more information, see *dhcp-class*. • <DHCP-CLASS-NAME> – Sets the DHCP class.

Example

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#address 192.168.13.4
class
 dhcpclass1

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  address 192.168.13.4 class dhcpclass1
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands:

no	Removes the DHCP pool's configured IP addresses
dhcp-class	Creates and configures the DHCP class parameters
alias	Creates and configures a network, VLAN, host, string, and network-service aliases

bootfile

dhcp-pool-mode commands

The Bootfile command provides a diskless node path to the image file while booting up. Only one file can be configured for each DHCP pool.

For more information on the BOOTP protocol with reference to the DHCP policy, see *bootp*.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
bootfile <IMAGE-FILE-PATH>
```

Parameters

```
bootfile <IMAGE-FILE-PATH>
```

<IMAGE-FILE-PATH>	Sets the path to the boot image for BOOTP clients. The file name can contain letters, numbers, dots and hyphens. Consecutive dots and hyphens are not permitted.

Example

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#bootfile test.txt

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  address 192.168.13.4 class dhcpclass1
  bootfile test.txt
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands:

no	Resets the boot image path for BOOTP clients
bootp	Configures BOOTP protocol parameters

ddns

dhcp-pool-mode commands

Configures *Dynamic Domain Name Service* (DDNS) parameters. Dynamic DNS provides a way to access an individual device in a DHCP serviced network using a static device name.

Depending on the DHCP server's configuration, the IP address of a device changes periodically. To ensure continuous accessibility to a device (having a dynamic IP address), the device's current IP address is published to a DDNS server that resolves the static device name (used to access the device) with a changing IP address.

The DDNS server must be accessible from outside the network and must be configured as an address resolver.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
ddns [domainname|multiple-user-class|server|ttl]

ddns domainname <DDNS-DOMAIN-NAME>
ddns multiple-user-class
ddns server [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
ddns ttl <1-864000>
```

Parameters

```
ddns domainname <DDNS-DOMAIN-NAME>
```

domainname <DDNS-DOMAIN-NAME>	Sets the domain name used for DNS updates The controller uses DNS to convert human readable host names into IP addresses. Host names are not case sensitive and can contain alphabetic or numeric letters or a hyphen. A *Fully Qualified Domain Name* (FQDN) consists of a host name plus a domain name. For example, computername.domain.com.

`ddns multiple-user-class`

multiple-user-class	Enables the multiple user class options with this DDNS domain

`ddns server [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}`

server	Configures the DDNS server used by this DHCP profile
[<IP>|<HOST-ALIAS-NAME>]	Configures the primary DDNS server. This is the default server. Use one of the following options to specify the primary DDNS server: • <IP> – Specifies the primary DDNS server's IP address • <HOST-ALIAS-NAME> – Specifies a host alias, mapped to the primary DDNS server's IP address. The host alias should be existing and configured. A network host alias maps a name to a single network host. For example, 'alias host $HOST 1.1.1.100'. In this example the host alias is '*$HOST*' and it maps to a single host '*1.1.1.100*'. For more information, see *alias*.
{<IP1>|<HOST-ALIAS-NAME1>}	Optional. Configures the secondary DDNS server. If the primary server is not reachable, this server is used. Use one of the following options to identify the secondary DDNS server: • <IP> – Specifies the secondary DDNS server's IP address • <HOST-ALIAS-NAME> – Specifies a host alias, mapped to the secondary DDNS server's IP address. The host alias should be existing and configured.

`ddns ttl <1-864000>`

ttl <1-864000>	Configures the *Time To Live* (TTL) value for DDNS updates • <1-86400> – Specify a value from 1- 864000 seconds.

Example

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#ddns domainname WID

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#ddns
multiple-user-class

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#ddns server
192.168.13.9

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  address 192.168.13.4 class dhcpclass1
  ddns server 192.168.13.9
  ddns domainname WID
  ddns multiple-user-class
  bootfile test.txt
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands:

no	Resets or disables a DHCP pool's DDNS settings

default-router

dhcp-pool-mode commands

Configures a default router or gateway IP address for a network pool

After a DHCP client has booted, the client begins sending packets to its default router. Set the IP address of one or a group of routers the controller uses to map host names into IP addresses available to DHCP supported clients. Up to 8 default router IP addresses are supported.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
default-router [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
```

Parameters

```
default-router [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
```

[<IP>|<HOST-ALIAS-NAME>]	Configures the primary default router, using one of the following options: • <IP> – Specifies the primary default router's IP address • <HOST-ALIAS-NAME> – Specifies a host alias, mapped to the primary default router's IP address
{<IP1>|<HOST-ALIAS-NAME1>}	Optional. Configures the secondary default router, using one of the following options: • <IP1> – Specifies the secondary default router's IP address • <HOST-ALIAS-NAME1> – Specifies a host alias, mapped to the secondary default router's IP address. If the primary default router is unavailable, the secondary router is used. A network host alias maps a name to a single network host. For example, 'alias host $HOST 1.1.1.100'. In this example the host alias is '*$HOST*' and it maps to a single host '*1.1.1.100*'. For more information, see *alias*. A maximum of 8 default routers can be configured.

Usage Guidelines:

The IP address of the router should be on the same subnet as the client subnet.

Example

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#default-router
192.168.13.8 192.168.13.9

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  address 192.168.13.4 class dhcpclass1
  ddns server 192.168.13.9
  ddns domainname WID
  ddns multiple-user-class
  bootfile test.txt
  default-router 192.168.13.8 192.168.13.9
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands:

no	Removes the default router settings

dns-server

dhcp-pool-mode commands

Configures a network's DNS server. The DNS server supports all clients connected to networks supported by the DHCP server.

For DHCP clients, the DNS server's IP address maps the hostname to an IP address. DHCP clients use the DNS server's IP address based on the order (sequence) configured.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
dns-server [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
```

Parameters

```
dns-server [<IP>|<HOST-ALIAS-NAME>] {<IP1> <HOST-ALIAS-NAME1>}
```

[<IP>|<HOST-ALIAS-NAME>]	Configures the primary DNS server, using one of the following options: • <IP> – Specifies the primary DNS server's IP address • <HOST-ALIAS-NAME> – Specifies a host alias, mapped to the primary DNS server's IP address A maximum of 8 DNS server's
{<IP1>|<HOST-ALIAS-NAME1>}	Optional. Configures the secondary DNS server, using one of the following options: • <IP1> – Specifies the secondary DNS server's IP address • <HOST-ALIAS-NAME1> – Specifies a host alias, mapped to the secondary DNS server's IP address. If the primary DNS server is unavailable, the secondary server is used. A network host alias maps a name to a single network host. For example, 'alias host $HOST 1.1.1.100'. In this example the host alias is '*$HOST*' and it maps to a single host '*1.1.1.100*'. For more information, see *alias*. A maximum of 8 DNS servers can be configured.

Example

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#dns-server
192.168.13.19

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  address 192.168.13.4 class dhcpclass1
  ddns server 192.168.13.9
  ddns domainname WID
  ddns multiple-user-class
  bootfile test.txt
  default-router 192.168.13.8 192.168.13.9
  dns-server 192.168.13.19
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands:

no	Removes DNS server settings

domain-name

dhcp-pool-mode commands

Sets the domain name for the DHCP pool

Provides the domain name used by the controller with this pool

Domain names are not case sensitive and can contain alphabetic or numeric letters or a hyphen. The FQDN consists of the host name and the domain name. For example, computername.domain.com.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
domain-name <DOMAIN-NAME>
```

Parameters

```
domain-name <DOMAIN-NAME>
```

<DOMAIN-NAME>	Defines the DHCP pool's domain name

Example

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#domain-name
documentation

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  address 192.168.13.4 class dhcpclass1
  ddns server 192.168.13.9
  ddns domainname WID
  ddns multiple-user-class
  domain-name documentation
  bootfile test.txt
  default-router 192.168.13.8 192.168.13.9
  dns-server 192.168.13.19
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands:

no	Removes a DHCP pool's domain name

excluded-address

dhcp-pool-mode commands

Identifies a single IP address or a range of IP addresses, included in the DHCP address pool, that cannot be assigned to clients by the DHCP server

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
excluded-address [<IP>|<HOST-ALIAS-NAME>|range]

excluded-address <IP>
excluded-address <HOST-ALIAS-NAME>
excluded-address range [<START-IP>|<START-HOST-ALIAS-NAME>] [<END-IP>|
          <END-HOST-ALIAS-NAME>]
```

Parameters

`excluded-address <IP>`

<IP>	Adds a single IP address to the excluded address list

`excluded-address <HOST-ALIAS-NAME>`

<HOST-ALIAS-NAME>	Adds a host alias. The host alias is mapped to a host's IP address. The host identified by the host alias is added to the excluded address list. The host alias should be existing and configured. A network host alias maps a name to a single network host. For example, 'alias host $HOST 1.1.1.100'. In this example the host alias is *'$HOST'* and it maps to a single host '*1.1.1.100*'. For more information, see *alias*.

`excluded-address range [<START-IP>|<START-HOST-ALIAS-NAME>] [<END-IP>|<END-HOST-ALIAS-NAME>]`

range [<START-IP>| <START-HOST-ALIAS-NAME>] [<END-IP>| <END-HOST-ALIAS-NAME>]	Adds a range of IP addresses to the excluded address list. Use one of the following options to provide the first IP address in the range: • <START-IP> – Specifies the first IP address in the range • <START-HOST-ALIAS-NAME> – Specifies a host alias, mapped to the first IP address in the range Use one of the following options to provide the last IP address in the range: • <END-IP> – Specifies the last IP address in the range • <END-HOST-ALIAS-NAME> – Specifies a host alias, mapped to the last IP address in the range The host aliases should be existing and configured.

Example

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#excluded-address range
192.168.13.25 192.168.13.28

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  network 192.168.13.0/24
  address 192.168.13.4 class dhcpclass1
  ddns server 192.168.13.9
  ddns domainname WID
  ddns multiple-user-class
  excluded-address range 192.168.13.25 192.168.13.28
  domain-name documentation
  bootfile test.txt
  default-router 192.168.13.8 192.168.13.9
  dns-server 192.168.13.19
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands:

no	Removes the exclude IP addresses settings

lease

dhcp-pool-mode commands

A lease is the duration a DHCP issued IP address is valid. Once a lease expires, and if the lease is not renewed, the IP address is revoked and is available for reuse. Generally, before an IP lease expires, the client tries to get the same IP address issued for the next lease period. This feature is enabled by default, with a lease period of 24 hours (1 day).

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
lease [<0-365>|infinite]

lease infinite
lease <0-365> {0-23} {0-59} {0-59}
```

Parameters

```
lease infinite
```

infinite	The lease never expires (equal to a static IP address assignment)

```
lease <0-365> {<0-23>} {<0-59>} {<0-59>}
```

<0-365>	Configures the lease duration in days **NOTE:** Days may be 0 only when hours and/or minutes are greater than 0.
<0-23>	Optional. Sets the lease duration in hours
<0-59>	Optional. Sets the lease duration in minutes
<0-59>	Optional. Sets the lease duration in seconds

Usage Guidelines:

If lease parameter is not configured on the DHCP pool, the default is used. The default is 24 hours.

Example

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#lease 100 23 59 59

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  network 192.168.13.0/24
  address 192.168.13.4 class dhcpclass1
  lease 100 23 59 59
  ddns server 192.168.13.9
  ddns domainname WID
```

```
  ddns multiple-user-class
  excluded-address range 192.168.13.25 192.168.13.28
  domain-name documentation
  bootfile test.txt
  default-router 192.168.13.8 192.168.13.9
  dns-server 192.168.13.19
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands:

no	Resets values or disables the DHCP pool lease settings

netbios-name-server

dhcp-pool-mode commands

Configures the NetBIOS (WINS) name server's IP address. This server is used to resolve NetBIOS host names.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
netbios-name-server [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
```

Parameters

```
netbios-name-server [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
```

[<IP>|<HOST-ALIAS-NAME>]	Configures the primary NetBIOS name server, using one of the following options: • <IP> – Specifies the primary NetBIOS name server's IP address • <HOST-ALIAS-NAME> – Specifies a host alias, mapped to the primary NetBIOS name server's IP address
{<IP1>|<HOST-ALIAS-NAME1>}	Optional. Configures the secondary NetBIOS name server, using one of the following options: • <IP1> – Specifies the secondary NetBIOS name server's IP address • <HOST-ALIAS-NAME1> – Specifies a host alias, mapped to the secondary NetBIOS name server's IP address. If the primary NetBIOS name server is unavailable, the secondary server is used. A network host alias maps a name to a single network host. For example, 'alias host $HOST 1.1.1.100'. In this example the host alias is *'$HOST'* and it maps to a single host '*1.1.1.100*'. For more information, see *alias*.

Example

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#netbios-name-server
192.168.13.25

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  network 192.168.13.0/24
  address 192.168.13.4 class dhcpclass1
  lease 100 23 59 59
```

```
  ddns server 192.168.13.9
  ddns domainname WID
  ddns multiple-user-class
  excluded-address range 192.168.13.25 192.168.13.28
  domain-name documentation
  bootfile test.txt
  default-router 192.168.13.8 192.168.13.9
  dns-server 192.168.13.19
  netbios-name-server 192.168.13.25
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands:

no	Removes the NetBIOS name server settings

netbios-node-type

dhcp-pool-mode commands

Defines the predefined NetBIOS node type. The NetBIOS node type resolves NetBIOS names to IP addresses.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
netbios-node-type [b-node|h-node|m-node|p-node]
```

Parameters

```
netbios-node-type [b-node|h-node|m-node|p-node]
```

[b-node|h-node|m-node|p-node]	Defines the netbios node type • b-node – Sets the node type as broadcast. Uses broadcasts to query nodes on the network for the owner of a NetBIOS name. • h-node – Sets the node type as hybrid. Uses a combination of two or more nodes. • m-node – Sets the node type as mixed. A mixed node uses broadcasted queries to find a node, and failing that, queries a known p-node name server for the address. • p-node – Sets the node type as peer-to-peer. Uses directed calls to communicate with a known NetBIOS name server (such as a WINS server), for the IP address of a NetBIOS machine.

Example

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#netbios-node-type
b-node

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  network 192.168.13.0/24
  address 192.168.13.4 class dhcpclass1
  lease 100 23 59 59
  ddns server 192.168.13.9
```

```
  ddns domainname WID
  ddns multiple-user-class
  excluded-address range 192.168.13.25 192.168.13.28
  domain-name documentation
  netbios-node-type b-node
  bootfile test.txt
  default-router 192.168.13.8 192.168.13.9
  dns-server 192.168.13.19
  netbios-name-server 192.168.13.25
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands:

no	Removes the NetBIOS node type settings

network

dhcp-pool-mode commands

Configures the DHCP server's network settings

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
network [<IP/M>|<NETWORK-ALIAS-NAME>]
```

Parameters

```
network [<IP/M>|<NETWORK-ALIAS-NAME>]
```

<IP/M>	Configures the network number and mask (for example, 192.168.13.0/24)
<NETWORK-ALIAS-NAME>	Configures a network alias to identify the network number and mask • <NETWORK-ALIAS-NAME> – Specify the network alias name. It should be existing and configured. A network alias defines a single network address. For example, 'alias network $NET 1.1.1.0/24'. In this example, the network alias name is: *$NET* **and** the network it is mapped to is: *1.1.1.0/24*. For more information see, *alias*.

Example

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#network 192.168.13.0/24

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  network 192.168.13.0/24
  address 192.168.13.4 class dhcpclass1
  lease 100 23 59 59
  ddns server 192.168.13.9
  ddns domainname WID
  ddns multiple-user-class
  excluded-address range 192.168.13.25 192.168.13.28
  domain-name documentation
```

```
  netbios-node-type b-node
  bootfile test.txt
  default-router 192.168.13.8 192.168.13.9
  dns-server 192.168.13.19
  netbios-name-server 192.168.13.25
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands:

no	Removes the network number and mask configured for this DHCP pool

next-server

dhcp-pool-mode commands

Configures the next server in the boot process

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
next-server [<IP>|<HOST-ALIAS-NAME>]
```

Parameters

```
next-server [<IP>|<HOST-ALIAS-NAME>]
```

<IP>	Configures the next server's (the first server in the boot process) IP address
<HOST-ALIAS-NAME>	Configures a host alias, mapped to the next server's IP address • <HOST-ALIAS-NAME> – Specify the host alias name. It should be existing and configured. A host alias maps a name to a single network host. For example, 'alias host $HOST 1.1.1.100'. In this example the host alias is '*$HOST*' and it maps to a single host '*1.1.1.100*'. For more information, see *alias*.

Example

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#next-server
192.168.13.26

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  network 192.168.13.0/24
  address 192.168.13.4 class dhcpclass1
  lease 100 23 59 59
  ddns server 192.168.13.9
  ddns domainname WID
  ddns multiple-user-class
  excluded-address range 192.168.13.25 192.168.13.28
  domain-name documentation
  netbios-node-type b-node
  bootfile test.txt
  default-router 192.168.13.8 192.168.13.9
```

```
  dns-server 192.168.13.19
  netbios-name-server 192.168.13.25
  next-server 192.168.13.26
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands:

no	Removes the next server configuration settings

no

dhcp-pool-mode commands

Removes or resets this DHCP user pool's settings

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no
[address|bootfile|ddns|default-router|dns-server|domain-name|excluded-address
|

lease|netbios-name-server|netbios-node-type|network|next-server|option|
          respond-via-unicast|static-binding|static-route|update]

no [bootfile|default-router|dns-server|domain-name|lease|netbios-name-server|
          netbios-node-type|next-server|network|respond-via-unicast]


no address [<IP>|<HOST-ALIAS-NAME>|all]
no address range [<START-IP>|<START-HOST-ALIAS-NAME>]
[<END-IP>|<END-HOST-ALIAS-NAME>]

no ddns [domainname|multiple-user-class|server|ttl]

no excluded-address [<IP>|<HOST-ALIAS-NAME>]
no excluded-address range [<START-IP>|<START-HOST-ALIAS-NAME>] [<END-IP>|
          <END-HOST-ALIAS-NAME>]

no option <OPTION-NAME>

no static-binding client-identifier <CLIENT-IDENTIFIER>
no static-binding hardware-address <MAC>

no static-route <IP/MASK> <GATEWAY-IP>

no update dns {override}
```

Parameters

`no [bootfile|default-router|dns-server|domain-name|lease|netbios-name-server|netbios-node-type|next-server|network|respond-via-unicast]`

no bootfile	Removes a BOOTP bootfile configuration
no default-router	Removes the configured default router for the DHCP pool
no dns-server	Removes the configured DNS server for the DHCP pool
no domain-name	Removes the configured DNS domain name
no lease	Resets the lease to its default (24 hours)
no netbios-name-server	Removes the configured NetBIOS name server
no netbios-node-type	Removes the NetBIOS node type
no next-server	Removes the next server utilized in the boot process
no network	Removes the DHCP server network information
no respond-via-unicast	Sets the DHCP offer and ACK as broadcast instead of unicast

`no address [<IP>|<HOST-ALIAS-NAME>|all]`

no address	Resets configured DHCP pool addresses
<IP>	Removes an IP address from the list of addresses
<HOST-ALIAS-NAME>	Removes the host alias (used to identify a single host) associated with this DHCP pool's address list
all	Removes configured DHCP IP addresses

`no address range [<START-IP>|<START-HOST-ALIAS-NAME>] [<END-IP>|<END-HOST-ALIAS-NAME>]`

no address	Resets the DHCP pool addresses
range [<START-IP>| <START-HOST-ALIAS-NAME>] [<END-IP>| <END-HOST-ALIAS-NAME>]	Removes a range of IP addresses and host aliases associated with this DHCP pool's address list. • <START-IP> – Specify the first IP address in the range. • <START-HOST-ALIAS-NAME> – Specify the host alias, mapped to the first IP address in the range. • <END-IP> – Specify the last IP address in the range. • <END-HOST-ALIAS-NAME> – Specify the host alias, mapped to the last IP address in the range. The specified IP addresses and host aliases are removed from the DHCP pool's address list.

`no ddns [domainname|multiple-user-class|server|ttl]`

no ddns	Resets DDNS parameters
domainname	Removes DDNS domain name information
multiple-user-class	Resets the use of a multiple user class with the DDNS
server	Removes configured DDNS servers
ttl	Resets the TTL information for DDNS updates

`no excluded-address [<IP>|<HOST-ALIAS-NAME>]`

no excluded-address <IP>	Removes an excluded IP address from the list of addresses that cannot be issued by the DHCP server • <IP> – Specify the IP address.
<HOST-ALIAS-NAME>	Removes the host alias (used to identify a single host) associated with this DHCP pool's excluded-address list

```
no excluded-address range [<START-IP>|<START-HOST-ALIAS-NAME>]
[<END-IP>|<END-HOST-ALIAS-NAME>]
```

no excluded-address	Removes a range of excluded IP addresses from the list of addresses that cannot be issued by the DHCP server
range [<START-IP>|<START-HOST-ALIAS-NAME>] [<END-IP>| <END-HOST-ALIAS-NAME>]	Removes a range of IP addresses and host aliases associated with this DHCP pool's excluded address list. • <START-IP> – Specify the first IP address in the range. • <START-HOST-ALIAS-NAME> – Specify the host alias, mapped to the first IP address in the range. • <END-IP> – Specify the last IP address in the range. • <END-HOST-ALIAS-NAME> – Specify the host alias, mapped to the last IP address in the range. The specified IP addresses and host aliases are removed from the DHCP pool's excluded address list.

```
no option <OPTION-NAME>
```

no option	Resets DHCP option information
<OPTION-NAME>	Defines the DHCP option

```
no static-binding client-identifier <CLIENT-IDENTIFIER>
```

no static-binding	Removes static bindings for DHCP client
client-identifier <CLIENT-IDENTIFIER>	Resets client identifier information • <CLIENT-IDENTIFIER> – Specify the client identifier.

```
no static-binding hardware-address <MAC>
```

no static-binding	Removes static bindings for a DHCP client
hardware-address <MAC>	Resets information based on the hardware address • <MAC> – Specify the hardware MAC address.

```
no static-route <IP/MASK> <GATEWAY-IP>
```

no static-route	Removes static routes for this DHCP pool
<IP/MASK>	Removes routing information for a particular subnet
<GATEWAY-IP>	Removes the gateway information from a particular subnet's routing information

```
no update dns {override}
```

no update dns	Removes DDNS settings
override	Optional. Removes DDNS updates from an onboard DHCP server

Example

```
The following example shows the DHCP pool settings before the 'no' commands
are executed:

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  network 192.168.13.0/24
  address 192.168.13.4 class dhcpclass1
  lease 100 23 59 59
  ddns server 192.168.13.9
  ddns domainname WID
  ddns multiple-user-class
  excluded-address range 192.168.13.25 192.168.13.28
  domain-name documentation
  netbios-node-type b-node
```

```
  bootfile test.txt
  default-router 192.168.13.8 192.168.13.9
  dns-server 192.168.13.19
  netbios-name-server 192.168.13.25
  next-server 192.168.13.26
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#no bootfile
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#no network
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#no default-router
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#no next-server
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#no domain-name
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#no ddns domainname
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#no lease

The following example shows the DHCP pool settings after the 'no' commands are
executed:

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  address 192.168.13.4 class dhcpclass1
  ddns server 192.168.13.9
  ddns multiple-user-class
  excluded-address range 192.168.13.25 192.168.13.28
  netbios-node-type b-node
  dns-server 192.168.13.19
  netbios-name-server 192.168.13.25
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands:

address	Configures the DHCP server's IP address pool
bootfile	Configures the BOOTP boot file path
ddns	Configures DDNS for use with this DHCP pool
default-router	Configures default routers for this DHCP pool
dns-server	Configures default DNS servers for this DHCP pool
domain-name	Configures the DDNS domain name for this DHCP pool
excluded-address	Configures IP addresses assigned as static addresses
lease	Configures the DHCP lease settings
netbios-name-server	Configures the NetBIOS name server
netbios-node-type	Configures the NetBIOS node type
network	Configures the DHCP server's network settings
next-server	Configures the next server in the BOOTP boot process
option	Configures the DHCP option
respond-via-unicast	Configures how a DHCP request and ACK are sent
static-binding	Configure static binding information
static-route	Configures static routes installed on DHCP clients
update	Controls DDNS service usage

option

dhcp-pool-mode commands

Configures raw DHCP options. The DHCP option must be configured under the DHCP server policy. The options configured under the DHCP pool/DHCP server policy can also be used in static-bindings.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
option <OPTION-NAME> [<DHCP-OPTION-IP>|<DHCP-OPTION-ASCII>]
```

Parameters

```
option <OPTION-NAME> [<DHCP-OPTION-IP>|<DHCP-OPTION-ASCII>]
```

<OPTION-NAME>	Sets the name of the DHCP option
<DHCP-OPTION-IP>	Sets DHCP option as an IP address
<DHCP-OPTION-ASCII>	Sets DHCP option as an ASCII string

NOTE
An option name in ASCII format accepts backslash (\) as an input but is not displayed in the output (Use `show runnig config` to view the output). Use a double backslash to represent a single backslash.

Example

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#option option1
157.235.208.80

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  address 192.168.13.4 class dhcpclass1
  ddns server 192.168.13.9
  ddns multiple-user-class
  excluded-address range 192.168.13.25 192.168.13.28
  netbios-node-type b-node
  dns-server 192.168.13.19
  netbios-name-server 192.168.13.25
  option option1 157.235.208.80
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands:

no	Resets values or disables the DHCP pool option settings

respond-via-unicast

dhcp-pool-mode commands

Sends DHCP offer and acknowledgement as unicast messages

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
respond-via-unicast
```

Parameters

None

Example

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#respond-via-unicast

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  address 192.168.13.4 class dhcpclass1
  ddns server 192.168.13.9
  ddns multiple-user-class
  excluded-address range 192.168.13.25 192.168.13.28
  netbios-node-type b-node
  dns-server 192.168.13.19
  netbios-name-server 192.168.13.25
  option option1 157.235.208.80
  respond-via-unicast
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands:

no	Disables sending of a DHCP offer and DHCP Ack as unicast messages. When disabled, sends offer and acknowledgement as broadcast messages.

static-route

dhcp-pool-mode commands

Configures a static route for a DHCP pool. Static routes define a gateway for traffic intended for other networks. This gateway is always used when an IP address does not match any route in the network.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
static-route <IP/M> <IP>
```

Parameters

```
static-route <IP/M> <IP>
```

<IP/M>	Specifies the IP destination prefix (for example, 10.0.0.0/8)
<IP>	Specifies the gateway IP address

Example

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#static-route
192.168.13.0/
24 192.168.13.7

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  address 192.168.13.4 class dhcpclass1
  ddns server 192.168.13.9
  ddns multiple-user-class
  excluded-address range 192.168.13.25 192.168.13.28
  netbios-node-type b-node
  dns-server 192.168.13.19
  netbios-name-server 192.168.13.25
  option option1 157.235.208.80
  respond-via-unicast
  static-route 192.168.13.0/24 192.168.13.7
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands:

no	Removes static route settings

update

dhcp-pool-mode commands

Controls the use of the DDNS service

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
update dns {override}
```

Parameters

`update dns {override}`

dns {override}	Configures DDNS parameters • override – Optional. Enables DDNS updates on an onboard DHCP server

Usage Guidelines:

A DHCP client cannot perform updates for RR's A, TXT and PTR resource records. Use `update (dns)(override)`to enable the internal DHCP server to send DDNS updates for resource records. The DHCP server can override the client, even if the client is configured to perform the updates.

In the DHCP server's DHCP pool, FQDN is configured as the DDNS domain name. This is used internally in DHCP packets between the DHCP server and the DNS server.

Example

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#update dns override

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  address 192.168.13.4 class dhcpclass1
  update dns override
  ddns server 192.168.13.9
  ddns multiple-user-class
  excluded-address range 192.168.13.25 192.168.13.28
  netbios-node-type b-node
  dns-server 192.168.13.19
  netbios-name-server 192.168.13.25
  option option1 157.235.208.80
  respond-via-unicast
  static-route 192.168.13.0/24 192.168.13.7
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands:

no	Removes dynamic DNS service control

static-binding

dhcp-pool-mode commands

Configures static IP address information for a particular device. Static address binding is executed on the device's hostname, client identifier, or MAC address. Static bindings allow the configuration of client parameters, such as DHCP server, DNS server, default routers, fixed IP address etc.

The following table summarizes static binding configuration commands.

Command	Description	Reference
static-binding	Creates a static binding policy and enters its configuration mode	page 958
static-binding-mode commands	Invokes static binding configuration commands	page 961

static-binding

static-binding

Configures static address bindings

A static address binding is a collection of configuration parameters, including an IP address, associated with, or bound to, a DHCP client. Bindings are managed by DHCP servers. DHCP bindings automatically map a device MAC address to an IP address using a pool of DHCP supplied addresses. Static bindings assign IP addresses without creating numerous host pools with manual bindings. Static host bindings use a text file the DHCP server reads. It eliminates the need for a lengthy configuration file and reduces the space required to maintain address pools.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
static-binding [client-identifier <CLIENT>|hardware-address <MAC>]
```

Parameters

```
static-binding [client-identifier <CLIENT>|hardware-address <MAC>]
```

client-identifier <CLIENT>	Enables a static binding configuration for a client based on its client identifier (as provided by DHCP option 61 and its key value) • <CLIENT> – Specify the client identifier (DHCP option 61).
hardware-address <MAC>	Enables a static binding configuration for a client based on its MAC address • <MAC> – Specify the MAC address of the client.

Example

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#static-binding
client-identifier test

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  address 192.168.13.4 class dhcpclass1
  update dns override
  ddns server 192.168.13.9
  ddns multiple-user-class
  excluded-address range 192.168.13.25 192.168.13.28
  netbios-node-type b-node
  dns-server 192.168.13.19
  netbios-name-server 192.168.13.25
  option option1 157.235.208.80
  respond-via-unicast
  static-route 192.168.13.0/24 192.168.13.7
  static-binding client-identifier test
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#

rfs4000-229D58(config-dhcp-policy-test-pool-testPool-binding-test)#?
DHCP static binding Mode commands:
  bootfile             Boot file name
  client-name          Client name
  default-router       Default routers
  dns-server           DNS Servers
```

```
  domain-name          Configure domain-name
  ip-address           Fixed IP address for host
  netbios-name-server  NetBIOS (WINS) name servers
  netbios-node-type    NetBIOS node type
  next-server          Next server in boot process
  no                   Negate a command or set its defaults
  option               Raw DHCP options
  respond-via-unicast  Send DHCP offer and DHCP Ack as unicast messages
  static-route         Add static routes to be installed on dhcp clients

  clrscr               Clears the display screen
  commit               Commit all changes made in this session
  do                   Run commands from Exec mode
  end                  End current mode and change to EXEC mode
  exit                 End current mode and down to previous mode
  help                 Description of the interactive help system
  revert               Revert changes
  service              Service Commands
  show                 Show running system information
  write                Write running configuration to memory or terminal

rfs4000-229D58(config-dhcp-policy-test-pool-testPool-binding-test)#

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#static-binding
hardware-address
11-22-33-44-55-66
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-11-22-33-44-55-66)#
?
DHCP static binding Mode commands:
  bootfile             Boot file name
  client-name          Client name
  default-router       Default routers
  dns-server           DNS Servers
  domain-name          Configure domain-name
  ip-address           Fixed IP address for host
  netbios-name-server  NetBIOS (WINS) name servers
  netbios-node-type    NetBIOS node type
  next-server          Next server in boot process
  no                   Negate a command or set its defaults
  option               Raw DHCP options
  respond-via-unicast  Send DHCP offer and DHCP Ack as unicast messages
  static-route         Add static routes to be installed on dhcp clients

  clrscr               Clears the display screen
  commit               Commit all changes made in this session
  do                   Run commands from Exec mode
  end                  End current mode and change to EXEC mode
  exit                 End current mode and down to previous mode
  help                 Description of the interactive help system
  revert               Revert changes
  service              Service Commands
  show                 Show running system information
  write                Write running configuration to memory or terminal

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-11-22-33-44-55-66)#
```

Related Commands:

no	Resets values or disables the DHCP policy static binding settings
static-binding-mode commands	Invokes static binding configuration commands

static-binding-mode commands

static-binding

The following table summarizes static binding configuration mode commands.

Command	Description	Reference
bootfile	Assigns a Bootfile name for the DHCP configuration on the network pool	page 961
client-name	Configures a client name	page 962
default-router	Configures default router or gateway IP address	page 963
dns-server	Sets the DNS server's IP address available to all DHCP clients connected to the DHCP pool	page 964
domain-name	Sets the network pool's domain name	page 965
ip-address	Configures a host's fixed IP address	page 965
netbios-name-server	Configures a NetBIOS (WINS) name server IP address	page 966
netbios-node-type	Defines the NetBIOS node type	page 967
next-server	Specifies the next server used in the boot process	page 968
no	Negates a command or sets its default	page 969
option	Configures raw DHCP options	page 971
respond-via-unicast	Sends a DHCP offer and DHCP Ack as unicast messages	page 972
static-route	Adds static routes installed on DHCP clients	page 973

bootfile

static-binding-mode commands

The Bootfile command provides a diskless node the path to the image file used while booting up. Only one file can be configured for each static IP binding.

For more information on the BOOTP protocol with reference to static binding, see *bootp*.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
bootfile <IMAGE-FILE-PATH>
```

Parameters

```
bootfile <IMAGE-FILE-PATH>
```

<IMAGE-FILE-PATH>	Sets the path to the boot image for BOOTP clients. The file name can contain letters, numbers, dots and hyphens. Consecutive dots and hyphens are not permitted.

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#bootfile
test.txt

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
  static-binding client-identifier test
   bootfile test.txt
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#
```

Related Commands:

no	Resets values or disables DHCP pool static binding settings
bootp	Configures BOOTP protocol parameters

client-name

static-binding-mode commands

Configures the client's name

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
client-name <NAME>
```

Parameters

```
client-name <NAME>
```

<NAME>	Specify the name of the client using this static IP address host pool. Do not include the domain name.

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#client-name
RFID

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
  static-binding client-identifier test
   client-name RFID
   bootfile test.txt
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#
```

Related Commands:

no	Resets values or disables DHCP pool static binding settings

default-router

static-binding-mode commands

Configures a default router or gateway IP address for the static binding configuration

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
default-router [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
```

Parameters

```
default-router [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
```

[<IP>|<HOST-ALIAS-NAME>]	Configures the primary default router, using one of the following options: • <IP> – Specifies the primary default router's IP address • <HOST-ALIAS-NAME> – Specifies a host alias, mapped to the primary default router's IP address
{<IP1>|<HOST-ALIAS-NAME1>}	Optional. Configures the secondary default router, using one of the following options: • <IP1> – Specifies the secondary default router's IP address • <HOST-ALIAS-NAME1> – Specifies a host alias, mapped to the secondary default router's IP address. If the primary default router is unavailable, the secondary router is used. A network host alias maps a name to a single network host. For example, 'alias host $HOST 1.1.1.100'. In this example the host alias is '$HOST' and it maps to a single host '1.1.1.100'. For more information, see alias.

Usage Guidelines:

The IP address of the router should be on the same subnet as the client subnet.

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#default-route
r 172.16.10.8 172.16.10.9

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
  static-binding client-identifier test
   client-name RFID
   bootfile test.txt
   default-router 172.16.10.8 172.16.10.9
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#
```

Related Commands:

no	Resets values or disables DHCP pool static binding settings

dns-server

static-binding-mode commands

Configures the DNS server for this static binding configuration. This DNS server supports the client for which the static binding has been configured.

For this client, the DNS server's IP address maps the host name to an IP address. DHCP clients use the DNS server's IP address based on the order (sequence) configured.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
dns-server [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
```

Parameters

```
dns-server [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
```

[<IP>|<HOST-ALIAS-NAME>]	Configures the primary DNS server, using one of the following options: • <IP> – Specifies the primary DNS server's IP address • <HOST-ALIAS-NAME> – Specifies a host alias, mapped to the primary DNS server's IP address
<HOST-ALIAS-NAME> <HOST-ALIAS-NAME1>	Configures the primary DNS server's host alias. The host alias is mapped to the DNS server's IP address, and should be existing and configured. • <HOST-ALIAS-NAME1> – Optional. Configures the secondary DNS server's host alias (if configured). If the primary DNS server is unavailable, the secondary DNS server is used. A network host alias maps a name to a single network host. For example, 'alias host $HOST 1.1.1.100'. In this example the host alias is '*$HOST*' and it maps to a single host '*1.1.1.100*'. For more information, see *alias*.
{<IP1>|<HOST-ALIAS-NAME1>}	Optional. Configures the secondary DNS server, using one of the following options: • <IP1> – Specifies the secondary DNS server's IP address • <HOST-ALIAS-NAME1> – Specifies a host alias, mapped to the secondary DNS server's IP address. If the primary DNS server is unavailable, the secondary DNS server is used. A network host alias maps a name to a single network host. For example, 'alias host $HOST 1.1.1.100'. In this example the host alias is '$HOST' and it maps to a single host '1.1.1.100'. For more information, see *alias*.

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#dns-server
172.16.10.7

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
  static-binding client-identifier test
   client-name RFID
   bootfile test.txt
   default-router 172.16.10.8 172.16.10.9
   dns-server 172.16.10.7
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#
```

Related Commands:

no	Resets values or disables DHCP pool static binding settings

domain-name

static-binding-mode commands

Sets the domain name for the static binding configuration

Domain names are not case sensitive and contain alphabetic or numeric letters (or a hyphen). A fully qualified domain name (FQDN) consists of a host name plus a domain name. For example, computername.domain.com

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
domain-name <DOMAIN-NAME>
```

Parameters

```
domain-name <DOMAIN-NAME>
```

<DOMAIN-NAME>	Defines the domain name for the static binding configuration

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#domain-name
documentation

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
  static-binding client-identifier test
   client-name RFID
   domain-name documentation
   bootfile test.txt
   default-router 172.16.10.8 172.16.10.9
   dns-server 172.16.10.7
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#
```

Related Commands:

no	Resets values or disables the DHCP pool static binding settings

ip-address

static-binding-mode commands

Configures a fixed IP address for a host

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
ip-address [<IP>|<HOST-ALIAS-NAME>]
```

Parameters

```
ip-address [<IP>|<HOST-ALIAS-NAME>]
```

<IP>	Configures a fixed IP address (in dotted decimal format) of the client using this host pool
<HOST-ALIAS-NAME>	Configures a host alias identifying the fixed IP address of the client using this host pool A network host alias maps a name to a single network host. For example, 'alias host $HOST 1.1.1.100'. In this example the host alias is '*$HOST*' and it maps to a single host '*1.1.1.100*'. For more information, see *alias*.

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#ip-address
172.16.10.9

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
  static-binding client-identifier test
   ip-address 172.16.10.9
   client-name RFID
   domain-name documentation
   bootfile test.txt
   default-router 172.16.10.8 172.16.10.9
   dns-server 172.16.10.7
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#
```

Related Commands:

no	Resets values or disables DHCP pool static binding settings

netbios-name-server

static-binding-mode commands

Configures the NetBIOS (WINS) name server's IP address. This server is used to resolve NetBIOS host names.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
netbios-name-server [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
```

Parameters

```
netbios-name-server [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
```

[<IP>|<HOST-ALIAS-NAME>]	Configures the primary NetBIOS server, using one of the following options: • <IP> – Specifies the primary NetBIOS name server's IP address • <HOST-ALIAS-NAME> – Specifies a host alias, mapped to the primary NetBIOS name server's IP address
{<IP1>|<HOST-ALIAS-NAME1>}	Optional. Configures the secondary NetBIOS name server, using one of the following options: • <IP1> – Specifies the secondary NetBIOS name server's IP address • <HOST-ALIAS-NAME1> – Specifies a host alias, mapped to the secondary NetBIOS name server's IP address. If the primary NetBIOS name server is unavailable, the secondary server is used. A network host alias maps a name to a single network host. For example, 'alias host $HOST 1.1.1.100'. In this example the host alias is '$HOST' and it maps to a single host '1.1.1.100'. For more information, see *alias*.

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#netbios-name-
server 172.16.10.23

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
  static-binding client-identifier test
   ip-address 172.16.10.9
   client-name RFID
   domain-name documentation
   bootfile test.txt
   default-router 172.16.10.8 172.16.10.9
   dns-server 172.16.10.7
   netbios-name-server 172.16.10.23
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#
```

Related Commands:

no	Resets values or disables DHCP pool static binding settings

netbios-node-type

static-binding-mode commands

Configures different predefined NetBIOS node types. The NetBIOS node defines the way a device resolves NetBIOS names to IP addresses.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
netbios-node-type [b-node|h-mode|m-node|p-node]
```

Parameters

```
netbios-node-type [b-node|h-node|m-node|p-node]
```

[b-node|h-mode| m-node|p-node]	Defines the netbios node type • b-node – Sets the node type as broadcast. Uses broadcasts to query nodes on the network for the owner of a NetBIOS name. • h-node – Sets the node type as hybrid. Uses a combination of two or more nodes. • m-node – Sets the node type as mixed. A mixed node uses broadcasted queries to find a node, and failing that, queries a known p-node name server for the address. • p-node – Sets the node type as peer-to-peer. Uses directed calls to communicate with a known NetBIOS name server (such as a WINS server), for the IP address of a NetBIOS machine.

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#netbios-node-
type
b-node

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
  static-binding client-identifier test
   ip-address 172.16.10.9
   client-name RFID
   domain-name documentation
   netbios-node-type b-node
   bootfile test.txt
   default-router 172.16.10.8 172.16.10.9
   dns-server 172.16.10.7
   netbios-name-server 172.16.10.23
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#
```

Related Commands:

no	Resets values or disables DHCP pool static binding settings

next-server

static-binding-mode commands

Configures the next server utilized in the boot process

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
next-server [<IP>|<HOST-ALIAS-NAME>]
```

Parameters

```
next-server [<IP>||<HOST-ALIAS-NAME>]
```

<IP>	Configures the next server's (the first server in the boot process) IP address
<HOST-ALIAS-NAME>	Configures a host alias, mapped to the next server's IP address • <HOST-ALIAS-NAME> – Specify the host alias name. It should be existing and configured. A network host alias maps a name to a single network host. For example, 'alias host $HOST 1.1.1.100'. In this example the host alias is '*$HOST*' and it maps to a single host '*1.1.1.100*'. For more information, see *alias*.

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#next-server
172.16.10.24

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
  static-binding client-identifier test
   ip-address 172.16.10.9
   client-name RFID
   domain-name documentation
   netbios-node-type b-node
   bootfile test.txt
   default-router 172.16.10.8 172.16.10.9
   dns-server 172.16.10.7
   netbios-name-server 172.16.10.23
   next-server 172.16.10.24
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#
```

Related Commands:

no	Resets values or disables DHCP pool static binding settings

no

static-binding-mode commands

Negates or reverts static binding settings for the selected DHCP server policy

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no [bootfile|client-name|default-router|dns-server|domain-name|ip-address|

netbios-name-server|netbios-node-type|next-server|option|respond-via-unicast|
          static-route]

no option <OPTION-NAME>

no static-route <IP/MASK> <GATEWAY-IP>
```

Parameters

```
no
[bootfile|client-name|default-router|dns-server|domain-name|ip-address|netbio
s-name-server|netbios-node-type|next-server||respond-via-unicast]
```

no bootfile	Removes the BOOTP bootfile configuration
no client-name	Removes the client name from the static binding configuration
no default-router	Removes the default router from the static binding configuration
no dns-server	Removes the DNS server from the static binding configuration
no domain-name	Removes the DNS domain name
no ip-address	Removes IP addresses from the static binding configuration
no netbios-name-server	Removes the NetBIOS name server
no netbios-node-type	Removes the NetBIOS node type
no next-server	Removes the next server utilized in the boot process
no respond-via-unicast	Sets the DHCP offer and ACK as broadcast instead of unicast

```
no option <OPTION-NAME>
```

no option <OPTION-NAME>	Resets the DHCP option to the value specified by the <OPTION-NAME> parameter

```
no static-route <IP/MASK> <GATEWAY-IP>
```

no static-route	Removes static routes from the static binding configuration
<IP/MASK>	Removes information for a particular subnet
<GATEWAY-IP>	Removes gateway information from a particular subnet's routing information

Example

```
The following example shows the DHCP pool static binding settings before the
'no' commands are executed:

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
  static-binding client-identifier test
   ip-address 172.16.10.9
   client-name RFID
   domain-name documentation
   netbios-node-type b-node
   bootfile test.txt
   default-router 172.16.10.8 172.16.10.9
   dns-server 172.16.10.7
   netbios-name-server 172.16.10.23
   next-server 172.16.10.24
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#no bootfile
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#no ip-address
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#no
default-router
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#no dns-server

The following example shows the DHCP pool static binding settings after the
'no' commands are executed:

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
  static-binding client-identifier test
```

```
    client-name RFID
    domain-name documentation
    netbios-node-type b-node
    netbios-name-server 172.16.10.23
    next-server 172.16.10.24
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#
```

Related Commands:

bootfile	Configures the BOOTP boot file path
client-name	Configures a hots's name
default-router	Configures default routers for a DHCP pool
dns-server	Configures default DNS servers for a DHCP pool
domain-name	Configures the DDNS domain name for a DHCP pool
ip-address	Configures IP addresses assigned to a host
netbios-name-server	Configures the NetBIOS name server
netbios-node-type	Configures the NetBIOS node type
next-server	Configures the next server utilized in the BOOTP boot process
option	Configures the DHCP option
respond-via-unicast	Configures the DHCP request and ACK sending mode (broadcast or unicast)
static-route	Configures the static binding's route

option

static-binding-mode commands

Configures the raw DHCP options in the DHCP policy. The DHCP options can be used only in static bindings.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
option <OPTION-NAME> [<DHCP-OPTION-IP>|<DHCP-OPTION-ASCII>]
```

Parameters

```
option <OPTION-NAME> [<DHCP-OPTION-IP>|<DHCP-OPTION-ASCII>]
```

<OPTION-NAME>	Sets the DHCP option name
<DHCP-OPTION-IP>	Sets the DHCP option as an IP address
<DHCP-OPTION-ASCII>	Sets the DHCP option as an ASCII string

Usage Guidelines:

Defines non standard DHCP option codes (0-254)

NOTE
An option name in ASCII format accepts a backslash (\) as an input, but is not displayed in the output (Use `show runnig config` to view the output). Use a double backslash to represent a single backslash.

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#option
option1 172.16.10.10

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
  static-binding client-identifier test
   client-name RFID
   domain-name documentation
   netbios-node-type b-node
   netbios-name-server 172.16.10.23
   next-server 172.16.10.24
   option option1 172.16.10.10
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#
```

respond-via-unicast

static-binding-mode commands

Sends a DHCP offer and DHCP acknowledge as unicast messages

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
respond-via-unicast
```

Parameters

None

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#respond-via-u
nicast

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
  static-binding client-identifier test
   client-name RFID
   domain-name documentation
   netbios-node-type b-node
   netbios-name-server 172.16.10.23
   next-server 172.16.10.24
   option option1 172.16.10.10
   respond-via-unicast
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#
```

Related Commands:

no	Resets values or disables DHCP pool static binding settings

static-route

static-binding-mode commands

Adds static routes to the static binding configuration

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
static-route <IP/MASK> <GATEWAY-IP>
```

Parameters

```
static-route <IP/MASK> <GATEWAY-IP>
```

<IP/MASK>	Sets the subnet for which the static route is configured
<GATEWAY-IP>	Specify the gateway's IP address

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-1)#static-route
10.0.0.0/10 157.235.208.235

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
  static-binding client-identifier test
   client-name RFID
   domain-name documentation
   netbios-node-type b-node
   netbios-name-server 172.16.10.23
   next-server 172.16.10.24
   option option1 172.16.10.10
   respond-via-unicast
   static-route 10.0.0.0/10 157.235.208.235
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#
```

Related Commands:

no	Resets values or disables DHCP pool static route settings

no

dhcp-server-policy

Negates a command or sets its default. When used in the DHCP server configuration context, the 'no' command resets or reverts the DHCP server policy settings.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no [bootp|dhcp-class|dhcp-pool|option|ping]

no bootp ignore

no dhcp-class <DHCP-CLASS-NAME>

no dhcp-pool <DHCP-POOL-NAME>

no option <DHCP-OPTION>

no ping timeout
```

Parameters

`no bootp ignore`

no bootp	Removes the BOOTP specific configuration
ignore	Removes the DHCP server ignoring BOOTP requests

`no dhcp-class <DHCP-CLASS-NAME>`

no dhcp-class <DHCP-CLASS-NAME>	Removes a specified DHCP class • <DHCP-CLASS-NAME> – Specifies the DHCP class name

`no dhcp-pool <DHCP-POOL-NAME>`

no dhcp-pool <DHCP-POOL-NAME>	Removes a specified DHCP pool • <DHCP-POOL-NAME> – Specifies the DHCP pool name

`no option <DHCP-OPTION>`

no option	Removes a DHCP option
<DHCP-OPTION>	Sets the DHCP option

`no ping timeout`

no ping timeout	Resets the DHCP server ping timeout • timeout – Resets the timeout to its default

Example

```
The following example shows the DHCP policy ‘test’ settings before the ‘no’
commands are executed:

rfs7000-37FABE(config-dhcp-policy-test)#show context
dhcp-server-policy test
 bootp ignore
 dhcp-class dhcpclass1
```

```
 dhcp-pool pool1
  address 1.2.3.4 class dhcpclass1
  update dns override
  --More--
rfs7000-37FABE(config-dhcp-policy-test)#

rfs7000-37FABE(config-dhcp-policy-test)#no bootp ignore
rfs7000-37FABE(config-dhcp-policy-test)#no dhcp-class dhcpclass1
rfs7000-37FABE(config-dhcp-policy-test)#no dhcp-pool pool1

The following example shows the DHCP policy ‘test’ settings after the ‘no’
commands are executed:

rfs7000-37FABE(config-dhcp-policy-test)#show context
dhcp-server-policy test
rfs7000-37FABE(config-dhcp-policy-test)#
```

Related Commands:

bootp	Configures the BOOTP protocol parameters
dhcp-class	Configures the DHCP user class parameters
dhcp-pool	Configures the DHCP pool
option	Configures the DHCP options
ping	Configures the DHCP ping timeout

option

dhcp-server-policy

Configures raw DHCP options. The DHCP option has to be configured in the DHCP server policy. The options configured in the DHCP pool/DHCP server policy can also be used in static bindings.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
option <OPTION-NAME> <0-250> [ascii|hexstring|ip]
```

Parameters

```
option <OPTION-NAME> <0-250> [ascii|hexstring|ip]
```

<OPTION-NAME>	Configures the option name
<0-250>	Configures the DHCP option code from 0 - 250
ascii	Configures the DHCP option as an ASCII string

hexstring	Configures the DHCP option as a hexadecimal string
ip	Configures the DHCP option as an IP address

Usage Guidelines:

Defines non standard DHCP option codes (0-254)

NOTE
An option name in ASCII format accepts a backslash (\) as an input, but is not displayed in the output (Use `show runnig config` to view the output). Use a double backslash to represent a single backslash.

Example

```
rfs7000-37FABE(config-dhcp-policy-test)#option option1 200 ascii

rfs7000-37FABE(config-dhcp-policy-test)#show context
dhcp-server-policy test
 option option1 200 ascii
rfs7000-37FABE(config-dhcp-policy-test)#
```

Related Commands:

no	Removes DHCP server options

ping

dhcp-server-policy

Configures the DHCP server's ping timeout interval. The controller uses the timeout to intermittently ping and discover whether a client requested IP address is available or in use.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
ping timeout <1-10>
```

Parameters

```
ping timeout <1-10>
```

timeout <1-10>	Sets the ping timeout from 1 - 10 seconds. The default is 1 second.

Example

```
rfs7000-37FABE(config-dhcp-policy-test)#ping timeout 2

rfs7000-37FABE(config-dhcp-policy-test)#show context
dhcp-server-policy test
```

```
 ping timeout 2
 option option1 200 ascii
rfs7000-37FABE(config-dhcp-policy-test)#
```

Related Commands:

no	Resets the ping interval to 1 second

Chapter

FIREWALL-POLICY

14

This chapter summarizes the firewall policy commands in the CLI command structure.

A firewall protects a network from attacks and unauthorized access from outside the network. Simultaneously, it allows authorized users to access required resources. Firewalls work on multiple levels. Some work at layers 1, 2 and 3 to inspect each packet. The packet is either passed, dropped or rejected based on rules configured on the firewall.

Firewalls use application layer filtering to enforce compliance. These firewalls can understand applications and protocols and can detect if an unauthorized protocol is being used, or an authorized protocol is being abused in any malicious way.

The third set of firewalls, 'Stateful Firewalls', consider the placement of individual packets within each packet in the series of packets being transmitted. If there is a packet that does not fit into the sequence, it is automatically identified and dropped.

Use (config) instance to configure firewall policy commands. To navigate to the *config-fw-policy* instance, use the following commands:

```
<DEVICE>(config)#firewall-policy <POLICY-NAME>

rfs7000-37FABE(config)#firewall-policy test
rfs7000-37FABE(config-fw-policy-test)#?
Firewall policy Mode commands:
  acl-logging                    Log on flow creating traffic
  alg                            Enable ALG
  clamp                          Clamp value
  dhcp-offer-convert             Enable conversion of broadcast dhcp offers to
                                 unicast
  dns-snoop                      DNS Snooping
  firewall                       Wireless firewall
  flow                           Firewall flow
  ip                             Internet Protocol (IP)
  ip-mac                         Action based on ip-mac table
  logging                        Firewall enhanced logging
  no                             Negate a command or set its defaults
  proxy-arp                      Enable generation of ARP responses on behalf
                                 of another device
  stateful-packet-inspection-l2  Enable stateful packet inspection in layer2
                                 firewall
  storm-control                  Storm-control
  virtual-defragmentation        Enable virtual defragmentation for IPv4
                                 packets (recommended for proper functioning
                                 of firewall)

  clrscr                         Clears the display screen
  commit                         Commit all changes made in this session
  do                             Run commands from Exec mode
  end                            End current mode and change to EXEC mode
  exit                           End current mode and down to previous mode
  help                           Description of the interactive help system
  revert                         Revert changes
```

```
  service                          Service Commands
  show                             Show running system information
  write                            Write running configuration to memory or
                                   terminal
rfs7000-37FABE(config-fw-policy-test)#
```

firewall-policy

Table 12 summarizes default firewall policy configuration commands.

TABLE 12 Firewall-Policy-Config Commands

Command	Description	Reference
acl-logging	Enables logging on flow creating traffic	page 980
alg	Enables an algorithm	page 981
clamp	Sets a clamp value to limit TCP MSS to inner path-MTU for tunnelled packets	page 982
dhcp-offer-convert	Enables the conversion of broadcast DHCP offers to unicast	page 983
dns-snoop	Sets the timeout value for DNS entries	page 983
firewall	Configures the wireless firewall	page 984
flow	Defines a session flow timeout	page 985
ip	Sets an IP address for a selected device	page 986
ip-mac	Defines an action based on IP-MAC table	page 993
logging	Enables enhanced firewall logging	page 995
no	Negates a command or reverts settings to their default	page 996
proxy-arp	Enables the generation of ARP responses on behalf of another device	page 1003
stateful-packet-inspection-12	Enables stateful packets-inspection in layer 2 firewall	page 1003
storm-control	Defines storm control and logging settings	page 1004
virtual-defragmentation	Enables virtual defragmentation of IPv4 packets	page 1006
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

acl-logging

firewall-policy

Enables logging on flow creating traffic

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
acl-logging
```

Parameters

None

Example

```
rfs4000-229D58(config-fw-policy-test)#acl-logging
rfs4000-229D58(config-fw-policy-test)#

rfs4000-229D58(config-fw-policy-test)#no acl-logging
rfs4000-229D58(config-fw-policy-test)#

rfs4000-229D58(config-fw-policy-test)#show context
firewall-policy test
 no ip dos tcp-sequence-past-window
 no acl-logging
rfs4000-229D58(config-fw-policy-test)#
```

Related Commands:

no	Disables logging on flow creating traffic

alg

firewall-policy

Enables preconfigured algorithms supporting a particular protocol

The Firewall policy allows traffic filtering at the application layer using the *Application Layer Gateway* (ALG) feature

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
alg [dns|facetime|ftp|sccp|sip|tftp]
```

Parameters

```
alg [dns|facetime|ftp|sccp|sip|tftp]
```

alg	Enables preconfigured algorithms. The default is enabled.
dns	Enables the *Domain Name System* (DNS) algorithm. The default is enabled.
facetime	Enables the FaceTime algorithm. The default is enabled.
ftp	Enables the *File Transfer Protocol* (FTP) algorithm. The default is enabled.
sccp	Enables the *Skinny Call Control Protocol* (SCCP) algorithm. The default is enabled.
sip	Enables the *Session Initiation Protocol* (SIP) algorithm. The default is enabled.
tftp	Enables the *Trivial File Transfer Protocol* (TFTP) algorithm. The default is enabled.

Example

```
rfs7000-37FABE(config-fw-policy-test)#alg tftp
```

Related Commands:

no	Disables or resets a specified algorithm

clamp

firewall-policy

This option limits the TCP *Maximum Segment Size* (MSS) to the size of the *Maximum Transmission Unit* (MTU) discovered by path MTU discovery for the inner protocol. This ensures the packet traverses through the inner protocol without fragmentation.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
clamp tcp-mss
```

Parameters

```
clamp tcp-mss
```

tcp-mss	Limits the TCP MSS size to the MTU value of the inner protocol for tunneled packets

Example

```
rfs7000-37FABE(config-fw-policy-test)#clamp tcp-mss
```

Related Commands:

no	Disables limiting of the TCP MSS

dhcp-offer-convert

firewall-policy

Enables the conversion of broadcast DHCP offers to unicast. Converting DHCP broadcast traffic to unicast traffic can help reduce network traffic loads. This option is disabled by default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
dhcp-offer-convert
```

Parameters

None

Example

```
rfs7000-37FABE(config-fw-policy-test)#dhcp-offer-convert

rfs7000-37FABE(config-fw-policy-test)#show context
firewall-policy test
 no ip dos tcp-sequence-past-window
 dhcp-offer-convert
rfs7000-37FABE(config-fw-policy-test)#
```

Related Commands:

no	Disables the conversion of broadcast DHCP offers to unicast

dns-snoop

firewall-policy

Sets the timeout interval for DNS snoop table entries

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
dns-snoop entry-timeout <30-86400>
```

Parameters

```
dns-snoop entry-timeout <30-86400>
```

entry-timeout <30-86400>	Sets the DNS snoop table entry timeout interval from 30 - 86400 seconds. An entry is retained in the DNS snoop table only for the specified time, and is deleted once this time is exceeded. The default is 1,800 seconds.

Example

```
rfs7000-37FABE(config-fw-policy-test)#dns-snoop entry-timeout 35

rfs7000-37FABE(config-fw-policy-test)#show context
firewall-policy test
 no ip dos tcp-sequence-past-window
 dhcp-offer-convert
 dns-snoop entry-timeout 35
rfs7000-37FABE(config-fw-policy-test)#
```

Related Commands:

no	Removes the DNS snoop table entry timeout interval

firewall

firewall-policy

Enables a device's firewall

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
firewall enable
```

Parameters

```
firewall enable
```

firewall enable	Enables wireless firewalls

Example

```
rfs7000-37FABE(config-fw-policy-default)#firewall enable
rfs7000-37FABE(config-fw-policy-default)#
```

Related Commands:

no	Disables a device's firewall

flow

firewall-policy

Defines the session flow timeout interval for different packet types

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
flow [dhcp|timeout]

flow dhcp stateful

flow timeout [icmp|other|tcp|udp]
flow timeout [icmp|other] <1-32400>
flow timeout udp <15-32400>
flow timeout tcp
[close-wait|reset|setup|stateless-fin-or-reset|stateless-general]
          <1-32400>
flow timeout tcp established <15-32400>
```

Parameters

```
flow dhcp stateful
```

dhcp	Configures DHCP packet flow
stateful	Performs a stateful check on DHCP packets. This feature is enabled by default.

```
flow timeout [icmp|other] <1-32400>
```

timeout	Configures a packet timeout
icmp	Configures the timeout for ICMP packets. The default is 30 seconds.
other	Configures the timeout for packets other than ICPM, TCP, or UDP. The default is 30 seconds.
<1-32400>	Configures the timeout from 1 - 32400 seconds

```
flow timeout udp <15-32400>
```

timeout	Configures a packet timeout
udp	Configures the timeout for UDP packets. The default is 30 seconds.
<15-32400>	Configures the timeout from 15 - 32400 seconds

```
flow timeout tcp
[close-wait|reset|setup|stateless-fin-or-reset|stateless-general]
<1-32400>
```

timeout	Configures a packet timeout
tcp	Configures the timeout for TCP packets
close-wait	Configures the closed TCP flow timeout. The default is 10 seconds.
reset	Configures the reset TCP flow timeout. The default is 10 seconds.
setup	Configures the opening TCP flow timeout. The default is 10 seconds.
stateless-fin-or-reset	Configures stateless TCP flow timeout created with the FIN or RESET packets. The default is 10 seconds.
stateless-general	Configures the stateless TCP flow timeout. The default is 90 seconds (1m 30 s).
<1-32400>	Configures the timeout from 1 - 32400 seconds

```
flow timeout tcp established <15-32400>
```

timeout	Configures the packet timeout
tcp	Configures the timeout for TCP packets
established	Configures the established TCP flow timeout. The default is 5400 seconds.
<15-32400>	Configures the timeout from 15 - 32400 seconds

Example

```
rfs7000-37FABE(config-rw-policy-test)#flow timeout udp 10000
rfs7000-37FABE(config-rw-policy-test)#flow timeout icmp 16000
rfs7000-37FABE(config-rw-policy-test)#flow timeout other 16000
rfs7000-37FABE(config-rw-policy-test)#flow timeout tcp established 1500

rfs7000-37FABE(config-fw-policy-test)#show context
firewall-policy test
 no ip dos tcp-sequence-past-window
 flow timeout icmp 16000
 flow timeout udp 10000
 flow timeout tcp established 1500
 flow timeout other 16000
 dhcp-offer-convert
 dns-snoop entry-timeout 35
rfs7000-37FABE(config-fw-policy-test)#
```

Related Commands:

no	Removes session timeout intervals configured for different packet types

ip

firewall-policy

Configures *Internet Protocol* (IP) components

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
ip [dos|tcp]

ip dos
{ascend|broadcast-multicast-icmp|chargen|fraggle|ftp-bounce|invalid-protocol|

ip-ttl-zero|ipspoof|land|option-route|router-advt|router-solicit|smurf|snork|

tcp-bad-sequence|tcp-fin-scan|tcp-intercept|tcp-max-incomplete|tcp-null-scan|

tcp-post-syn|tcp-sequence-past-window|tcp-xmas-scan|tcphdrfrag|twinge|
          udp-short-hdr|winnuke}

ip dos
{ascend|broadcast-multicast-icmp|chargen|fraggle|ftp-bounce|invalid-protocol|

ip-ttl-zero|ipsproof|land|option-route|router-advt|router-solicit|smurf|snork
|

tcp-bad-sequence|tcp-fin-scan|tcp-intercept|tcp-null-scan|tcp-post-scan|

tcp-sequence-past-window|tcp-xmas-scan|tcphdrfrag|twinge|udp-short-hdr|winnuk
e}
          [log-and-drop|log-only] log-level
[<0-7>|alerts|critical|debugging|emergencies|
          errors|informational|notifications|warnings]

ip dos
{ascend|broadcast-multicast-icmp|chargen|fraggle|ftp-bounce|invalid-protocol|

ip-ttl-zero|ipsproof|land|option-route|router-advt|router-solicit|smurf|snork
|

tcp-bad-sequence|tcp-fin-scan|tcp-intercept|tcp-null-scan|tcp-post-scan|

tcp-sequence-past-window|tcp-xmas-scan|tcphdrfrag|twinge|udp-short-hdr|winnuk
e}
          [drop-only]

ip dos tcp-max-incomplete [high|low] <1-1000>

ip tcp
[adjust-mss|optimize-unnecessary-resends|recreate-flow-on-out-of-state-syn|

validate-icmp-unreachable|validate-rst-ack-number|validate-rst-seq-number]

ip tcp adjust-mss <472-1460>

ip tcp [optimize-unnecessary-resends|recreate-flow-on-out-of-state-syn|

validate-icmp-unreachable|validate-rst-ack-number|validate-rst-seq-number]
```

Parameters

```
ip dos {ascend|broadcast-multicast-icmp|chargen|fraggle|ftp-bounce|
invalid-protocol|ip-ttl-zero|ipsproof|land|option-route|router-advt|router-so
licit|
smurf|snork|tcp-bad-sequence|tcp-fin-scan|tcp-intercept|tcp-null-scan|tcp-pos
t-scan|
tcp-sequence-past-window|tcp-xmas-scan|tcphdrfrag|twinge|udp-short-hdr|winnuk
e}
[log-and-drop|log-only] log-level
[<0-7>|alerts|critical|debug|emergencies|errors|
informational|notifications|warnings]
```

dos	Identifies IP events as DoS events
ascend	Optional. Detects ASCEND DoS attacks Ascend DoS attacks target known vulnerabilities in various versions of Ascend routers. Ascend routers listen on UDP port 9 for packets from Ascend's Java Configurator. Sending a formatted packet to this port can cause an Ascend router to crash.
broadcast-multicast-icmp	Optional. Detects broadcast or multicast ICMP Dos attacks Broadcast or multicast ICMP DoS attacks take advantage of ICMP behavior in response to echo replies. These attacks spoof the source address of the target and send ICMP broadcast or multicast echo requests to the rest of the network, flooding the target machine with replies.
chargen	Optional. Detects Chargen attacks The Character Generation Protocol (chargen) is an IP suite service primarily used for testing and debugging networks. It is also used as a source of generic payload for bandwidth and QoS measurements. The Chargen attack establishes a Telnet connection to port 19 and attempts to use the character generator service to create a string of characters which is then directed to the DNS service on port 53 to disrupt DNS services.
fraggle	Optional. Detects Fraggle DoS attacks The Fraggle DoS attack uses a list of broadcast addresses to send spoofed UDP packets to each broadcast address' echo port (port 7). Each of those addresses that have port 7 open will respond to the request generating a lot of traffic on the network. For those that do not have port 7 open they will send an unreachable message back to the originator, further clogging the network with more traffic.
ftp-bounce	Optional. Detects FTP bounce attacks A FTP bounce attack is a MIM attack that enables an attacker to open a port on a different machine using FTP. FTP requires that when a connection is requested by a client on the FTP port (21), another connection must open between the server and the client. To confirm, the PORT command has the client specify an arbitrary destination machine and port for the data connection. This is exploited by the attacker to gain access to a device that may not be the originating client.
invalid-protocol	Optional. Enables a check for an invalid protocol number Attackers may use vulnerability in the endpoint implementation by sending invalid protocol fields, or may misuse the misinterpretation of endpoint software. This can lead to inadvertent leakage of sensitive network topology information, call hijacking, or a DoS attack.
ip-ttl-zero	Optional. Enables a check for the TCP/IP TTL field having a value of zero (0) The TCP IP TTL Zero DoS attack sends spoofed multicast packets onto the network which have a *Time to Live* (TTL) of 0. This causes packets to loop back to the spoofed originating machine, and can cause the network to overload.
ipsproof	Optional. Enables a check for the IP spoofing DoS attacks IP Spoof is a category of DoS attack that sends IP packets with forged source addresses. This can hide the identity of the attacker.
land	Optional. Detects LAND DoS attacks A *Local Area Network Denial* (LAND) is a DoS attack where IP packets are spoofed and sent to a device where the source IP and destination IP of the packet are the target device's IP, and similarly, the source port and destination port are open ports on the same device. This causes the attacked device to reply to itself continuously.

option-route	Optional. Enables an IP Option Record Route DoS check
router-advt	Optional. Detects router-advertisement attacks This attack uses ICMP to redirect the network router function to some other host. If that host can not provide router services, a DoS of network communications occurs as routing stops. This can also be modified to single out a specific system, so that only that system is subject to attack (because only that system sees the 'false' router). By providing router services from a compromised host, the attacker can also place themselves in a man-in-the-middle situation and take control of any open channel at will (as mentioned earlier, this is often used with TCP packet forgery and spoofing to intercept and change open TELNET sessions).
router-solicit	Optional. Detects router solicitation attacks The ICMP router solicitation scan is used to actively find routers on a network. A hacker could set up a protocol analyzer to detect routers as they broadcast routing information on the network. In some instances, however, routers may not send updates. For example, if the local network does not have other routers, the router may be configured to not send routing information packets onto the local network. ICMP offers a method for router discovery. Clients send ICMP router solicitation multicasts onto the network, and routers must respond (as defined in RFC 1122). (For more information about the process of ICMP router solicitation, see "Routing Sequences for ICMP.") By sending ICMP router solicitation packets (ICMP type 9) on the network and listening for ICMP router discovery replies (ICMP type 10), hackers can build a list of all of the routers that exist on a network segment. Hackers often use this scan to locate routers that do not reply to ICMP echo requests
smurf	Optional. In this attack, a large number of ICMP echo packets are sent with a spoofed source address. This causes the device with the spoofed source address to be flooded with a large number of replies.
snork	Optional. This attack causes a remote Windows™ NT to consume 100% of the CPU's resources. This attack uses a UDP packet with a destination port of 135 and a source port of 7, 9, or 135. This attack can also be exploited as a bandwidth consuming attack.
tcp-bad-sequence	Optional. A DoS attack that uses a specially crafted TCP packet to cause the targeted device to drop all subsequent network traffic for a specific TCP connection
tcp-fin-scan	Optional. Detects TCP FIN scan attacks Hackers use the TCP FIN scan to identify listening TCP port numbers based on how the target device reacts to a transaction close request for a TCP port (even though no connection may exist before these close requests are made). This type of scan can get through basic firewalls and boundary routers that filter on incoming TCP packets with the *Finish* (FIN) and ACK flag combination. The TCP packets used in this scan include only the TCP FIN flag setting. If the target device's TCP port is closed, the target device sends a TCP RST packet in reply. If the target device's TCP port is open, the target device discards the FIN and sends no reply.

tcp-intercept	Optional. Prevents TCP intercept attacks by using TCP SYN cookies A SYN-flooding attack occurs when a hacker floods a server with a barrage of requests for connection. Because these messages have unreachable return addresses, the connections cannot be established. The resulting volume of unresolved open connections eventually overwhelms the server and can cause it to deny service to valid requests, thereby preventing legitimate users from connecting to a Web site, accessing e-mail, using FTP service, and so on. The TCP intercept feature helps prevent SYN-flooding attacks by intercepting and validating TCP connection requests. In intercept mode, the TCP intercept software intercepts TCP *synchronization* (SYN) packets from clients to servers that match an extended access list. The software establishes a connection with the client on behalf of the destination server, and if successful, establishes the connection with the server on behalf of the client and knits the two half-connections together transparently. Thus, connection attempts from unreachable hosts will never reach the server. The software continues to intercept and forward packets throughout the duration of the connection. The number of SYNs per second and the number of concurrent connections proxied depends on the platform, memory, processor, and other factors. In the case of illegitimate requests, the software's aggressive timeouts on half-open connections and its thresholds on TCP connection requests protect destination servers while still allowing valid requests. When establishing a security policy using TCP intercept, you can choose to intercept all requests or only those coming from specific networks or destined for specific servers. You can also configure the connection rate and threshold of outstanding connections. Optionally operate TCP intercept in watch mode, as opposed to intercept mode. In watch mode, the software passively watches the connection requests flowing through the router. If a connection fails to get established in a configurable interval, the software intervenes and terminates the connection attempt.
tcp-null-scan	Optional. Detects TCP NULL scan attacks Hackers use the TCP NULL scan to identify listening TCP ports. This scan also uses a series of strangely configured TCP packets, which contain a sequence number of 0 and no flags. Again, this type of scan can get through some firewalls and boundary routers that filter incoming TCP packets with standard flag settings. If the target device's TCP port is closed, the target device sends a TCP RST packet in reply. If the target device's TCP port is open, the target discards the TCP NULL scan, sending no reply.
tcp-post-syn	Optional. Detects TCP post SYN DoS attacks A remote attacker may be attempting to avoid detection by sending a SYN frame with a different sequence number than the original SYN. This can cause an *Intrusion Detection System* (IDS) to become unsynchronized with the data in a connection. Subsequent frames sent during the connection are ignored by the IDS.
tcp-sequence-past-window	Optional. Enables a TCP SEQUENCE PAST WINDOW DoS attack check. Disable this check to work around a bug in Windows XP's TCP stack which sends data past the window when conducting a selective ACK.
tcp-xmas-scan	Optional. A TCP XMAS scan finds services on ports. A closed port returns a RST. This allows the attacker to identify open ports.
tcphdrfrag	Optional. A DoS attack where the TCP header spans IP fragments
twinge	Optional. A twinge attack is a flood of false ICMP packets to try and slow down a system
udp-short-hdr	Optional. Enables the identification of truncated UDP headers and UDP header length fields
winnuke	Optional. This DoS attack is specific to Windows™ 95 and Windows™ NT. The WINNUKE DoS attack sends a large amount of data to UDP port 137 to crash the NETBIOS service on windows and results in high CPU utilization on the target machine.
log-and-drop	Logs the event and drops the packet
log-only	Logs the event only, the packet is not dropped
log-level	Configures the log level
<0-7>	Sets the numeric logging level
emergencies	Numerical severity 0. System is unusable

alerts	Numerical severity 1. Indicates a condition where immediate action is required
critical	Numerical severity 2. Indicates a critical condition
errors	Numerical severity 3. Indicates an error condition
warnings	Numerical severity 4. Indicates a warning condition
notification	Numerical severity 5. Indicates a normal but significant condition
informational	Numerical severity 6. Indicates a informational condition
debugging	Numerical severity 7. Debugging messages

`ip dos`
`{ascend|broadcast-multicast-icmp|chargen|fraggle|ftp-bounce|invalid-protocol|ip-ttl-zero|ipsproof|land|option-route|router-advt|router-solicit|smurf|snork|tcp-bad-sequence|tcp-fin-scan|tcp-intercept|tcp-null-scan|tcp-post-scan|tcp-sequence-past-window|tcp-xmas-scan|tcphdrfrag|twinge|udp-short-hdr|winnuke}`
`[drop-only]`

dos	Identifies IP events as DoS events
ascend	Optional. Enables an ASCEND DoS check. Ascend routers listen on UDP port 9 for packets from Ascend's Java Configurator. Sending a formatted packet to this port can cause an Ascend router to crash.
broacast-multicast-icmp	Optional. Detects broadcast or multicast ICMP packets as an attack
chargen	Optional. The *Character Generation Protocol* (chargen) is an IP suite service primarily used for testing and debugging networks. It is also used as a source of generic payload for bandwidth and QoS measurements.
fraggle	Optional. A Fraggle DoS attack checks for UDP packets to or from port 7 or 19
ftp-bounce	Optional. A FTP bounce attack is a MIM attack that enables an attacker to open a port on a different machine using FTP. FTP requires that when a connection is requested by a client on the FTP port (21), another connection must open between the server and the client. To confirm, the PORT command has the client specify an arbitrary destination machine and port for the data connection. This is exploited by the attacker to gain access to a device that may not be the originating client.
invalid-protocol	Optional. Enables a check for invalid protocol number
ip-ttl-zero	Optional. Enables a check for the TCP/IP TTL field having a value of zero (0)
ipsproof	Optional. Enables a check for IP spoofing DoS attack
land	Optional. A *Local Area Network Denial* (LAND) is a DoS attack where IP packets are spoofed and sent to a device where the source IP and destination IP of the packet are the target device's IP, and similarly, the source port and destination port are open ports on the same device. This causes the attacked device to reply to itself continuously.
option-route	Optional. Enables an IP Option Record Route DoS check
router-advt	Optional. This is an attack, where a default route entry is added remotely to a device. This route entry is given preference, and thereby exposes an attack vector.
router-solicit	Optional. Router solicitation messages are sent to locate routers as a form of network scanning. This information can then be used to attack a device.
smurf	Optional. In this attack, a large number of ICMP echo packets are sent with a spoofed source address. This causes the device with the spoofed source address to be flooded with a large number of replies.
snork	Optional. This attack causes a remote Windows™ NT to consume 100% of the CPU's resources. This attack uses a UDP packtet with a destination port of 135 and a source port of 7, 9, or 135. This attack can also be exploited as a bandwidth consuming attack.
tcp-bad-sequence	Optional. A DoS attack that uses a specially crafted TCP packet to cause the targeted device to drop all subsequent network traffic for a specific TCP connection

tcp-fin-scan	Optional. A FIN scan finds services on ports. A closed port returns a RST. This allows the attacker to identify open ports.
tcp-intercept	Optional. Prevents TCP intercept attacks by using TCP SYN cookies
tcp-null-scan	Optional. A TCP null scan finds services on ports. A closed port returns a RST. This allows the attacker to identify open ports
tcp-post-syn	Optional. Enables a TCP post SYN DoS attack
tcp-sequence-past-window	Optional. Enables a TCP SEQUENCE PAST WINDOW DoS attack check. Disable this check to work around a bug in Windows XP's TCP stack which sends data past the window when conducting a selective ACK.
tcp-xmas-scan	Optional. A TCP XMAS scan finds services on ports. A closed port returns a RST. This allows the attacker to identify open ports.
tcphdrfrag	Optional. A DoS attack where the TCP header spans IP fragments
twinge	Optional. A twinge attack is a flood of false ICMP packets to try and slow down a system
udp-short-hdr	Optional. Enables the identification of truncated UDP headers and UDP header length fields
winnuke	Optional. This DoS attack is specific to Windows™ 95 and Windows™ NT, causing devices to crash with a blue screen
drop-only	Optional. Drops a packet without logging

```
ip dos tcp-max-incomplete [high|low] <1-1000>
```

dos	Identifies IP events as DoS events
tcp-max-incomplete	Sets the limits for the maximum number of incomplete TCP connections
high	Sets the upper limit for the maximum number of incomplete TCP connections
low	Sets the lower limit for the maximum number of incomplete TCP connections
<1-1000>	Sets the range limit from 1 - 1000 connections

```
ip tcp adjust-mss <472-1460>
```

tcp	Identifies and configures TCP events and configuration items
adjust-mss	Adjusts the TCP *Maximum Segment Size* (MSS). Use this option to adjust the MSS for TCP segments on the router.
<472-1460>	Sets the TCP MSS value from 472 - 1460 bytes. The default is 472 bytes.

```
ip tcp [optimize-unnecessary-resends|recreate-flow-on-out-of-state-syn|
validate-icmp-unreachable|validate-rst-ack-number|validate-rst-seq-number]
```

tcp	Identifies and configures TCP events and configuration items
optimize-unnecessary-resends	Enables the validation of unnecessary TCP packets
recreate-flow-on-out-of-state-sync	Allows a TCP SYN packet to delete an old flow in TCP_FIN_FIN_STATE, and TCP_CLOSED_STATE states and create a new flow
validate-icpm-unreachable	Enables the validation of the sequence number in ICMP unreachable error packets, which abort an established TCP flow
validate-rst-ack-number	Enables the validation of the acknowledgment number in RST packets, which abort a TCP flow
validate-rst-seq-number	Enables the validation of the sequence number in RST packets, which abort an established TCP flow

Example

```
rfs7000-37FABE(config-rw-policy-test)#ip dos fraggle drop-only
```

```
rfs7000-37FABE(config-rw-policy-test)#ip dos tcp-max-incomplete high 600
rfs7000-37FABE(config-rw-policy-test)#ip dos tcp-max-incomplete low 60
rfs7000-37FABE(config-fw-policy-test)#ip dos tcp-sequence-past-window
drop-only

rfs7000-37FABE(config-fw-policy-test)#show context
firewall-policy test
 ip dos fraggle drop-only
 ip dos tcp-sequence-past-window drop-only
 ip dos tcp-max-incomplete high 600
 ip dos tcp-max-incomplete low 60
 flow timeout icmp 16000
 flow timeout udp 10000
 flow timeout tcp established 1500
 flow timeout other 16000
 dhcp-offer-convert
 dns-snoop entry-timeout 35
rfs7000-37FABE(config-fw-policy-test)#
```

Related Commands:

no	Resets firewall policy IP components

ip-mac

firewall-policy

Defines an action based on the device IP MAC table, and also detects conflicts between IP addresses and MAC addresses

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
ip-mac [conflict|routing]

ip-mac conflict drop-only
ip-mac conflict [log-and-drop|log-only] log-level
[<0-7>|alerts|critical|debug|
          emergencies|errors|informational|notifications|warnings]

ip-mac routing conflict drop-only
ip-mac routing [log-and-drop|log-only] log-level [<0-7>|alerts|critical|debug|
          emergencies|errors|informational|notifications|warnings]
```

Parameters

	`ip-mac conflict drop-only`
conflict	Action performed when a conflict exists between the IP address and MAC address. This option is enabled by default.
drop-only	Drops a packet without logging

	`ip-mac conflict [log-and-drop|log-only] log-level [<0-7>|alerts|critical|debug| emergencies|errors|informational|notifications|warnings]`
conflict	Action performed when a conflict exists between the IP address and MAC address. This option is enabled by default.
log-and-drop	Logs the event and drops the packet. This is the default setting.
log-only	Logs the event only, the packet is not dropped
log-level	Configures the log level
<0-7>	Sets the numeric logging level
alerts	Numerical severity 1. Indicates a condition where immediate action is required
critical	Numerical severity 2. Indicates a critical condition
debugging	Numerical severity 7. Debugging messages
emergencies	Numerical severity 0. System is unusable
errors	Numerical severity 3. Indicates an error condition
informational	Numerical severity 6. Indicates a informational condition
notification	Numerical severity 5. Indicates a normal but significant condition
warnings	Numerical severity 4. Indicates a warning condition. This is the default setting

	`ip-mac routing conflict drop-only`
routing	Enables IPMAC routing conflict detection. This is also known as a Hole-196 attack in the network. This feature helps to detect if the client is sending routed packets to the correct router-mac-address.
conflict	Defines the action performed when a routing table conflict is detected. This option is enabled by default.
drop-only	Drops a packet without logging

	`ip-mac routing [log-and-drop|log-only] log-level [<0-7>|alerts|critical|debug| emergencies|errors|informational|notifications|warnings]`
routing	Defines a routing table based action
conflict	Action performed when a conflict exists in the routing table. This option is enabled by default.
log-and-drop	Logs the event and drops the packet. This is the default setting.
log-only	Logs the event only, the packet is not dropped
log-level	Configures the log level to log this event under
<0-7>	Sets the numeric logging level
alerts	Numerical severity 1. Indicates a condition where immediate action is required
critical	Numerical severity 2. Indicates a critical condition
debugging	Numerical severity 7. Debugging messages
emergencies	Numerical severity 0. System is unusable
errors	Numerical severity 3. Indicates an error condition

informational	Numerical severity 6. Indicates a informational condition
notification	Numerical severity 5. Indicates a normal but significant condition
warnings	Numerical severity 4. Indicates a warning condition. This is the default setting.

Example

```
rfs7000-37FABE(config-rw-policy-test)#ip-mac conflict drop-only
rfs7000-37FABE(config-rw-policy-test)#ip-mac routing conflict log-and-drop
log-level notifications

rfs7000-37FABE(config-fw-policy-test)#show context
firewall-policy test
 ip dos fraggle drop-only
 ip dos tcp-sequence-past-window drop-only
 ip dos tcp-max-incomplete high 600
 ip dos tcp-max-incomplete low 60
 ip-mac conflict drop-only
 ip-mac routing conflict log-only log-level notifications
 flow timeout icmp 16000
 flow timeout udp 10000
 flow timeout tcp established 1500
 flow timeout other 16000
 dhcp-offer-convert
 dns-snoop entry-timeout 35
rfs7000-37FABE(config-fw-policy-test)#
```

Related Commands:

no	Disables actions based on device IP MAC table, IP address, and MAC address conflict detection

logging

firewall-policy

Configures enhanced firewall logging

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
logging [icmp-packet-drop|malformed-packet-drop|verbose]

logging verbose
logging [icmp-packet-drop|malformed-packet-drop] [all|rate-limited]
```

Parameters

```
logging verbose
```

logging	Configures enhanced firewall logging. This option is disabled by default.
verbose	Enables verbose logging

```
logging [icmp-packet-drop|malformed-packet-drop] [all|rate-limited]
```

logging	Configures enhanced firewall logging
icmp-packet-drop	Drops ICMP packets that do not pass sanity checks. The default is none.
malformed-packet-drop	Drops raw IP packets that do not pass sanity checks. The default is none.
all	Logs all messages
rate-limited	Enables rate-limited logging. This option sets the rate limit for log messages to one message every 20 seconds.

Example

```
rfs7000-37FABE(config-rw-policy-test)#logging verbose
rfs7000-37FABE(config-rw-policy-test)#logging icmp-packet-drop rate-limited
rfs7000-37FABE(config-rw-policy-test)#logging malformed-packet-drop all
rfs7000-37FABE(config-fw-policy-test)#show context
firewall-policy test
 ip dos fraggle drop-only
 ip dos tcp-sequence-past-window drop-only
 ip dos tcp-max-incomplete high 600
 ip dos tcp-max-incomplete low 60
 ip-mac conflict drop-only
 ip-mac routing conflict log-only log-level notifications
 flow timeout icmp 16000
 flow timeout udp 10000
 flow timeout tcp established 1500
 flow timeout other 16000
 dhcp-offer-convert
 logging icmp-packet-drop rate-limited
 logging malformed-packet-drop all
 logging verbose
 dns-snoop entry-timeout 35
rfs7000-37FABE(config-fw-policy-test)#
```

Related Commands:

no	Disables enhanced firewall logging

no

firewall-policy

Negates a command or sets the default for firewall policy commands

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no
[acl-logging|alg|clamp|dhcp-offer-convert|dns-snoop|firewall|flow|ip|ip-mac|l
ogging|

proxy-arp|stateful-packet-inspection-l2|storm-control|virtual-defragmentation
]

no [acl-logging|dhcp-offer-convert|proxy-arp|stateful-packet-inspection-l2]

no alg [dns|ftp|sip|tftp]

no clamp tcp-mss

no dns-snoop entry-timeout

no firewall enable

no flow dhcp stateful
no flow timeout [icmp|other|udp]
no flow timeout tcp
[closed-wait|established|reset|setup|stateless-fin-or-reset|
          stateless-general]

no ip dos {ascend|broadcast-multicast-icmp|chargen|fraggle|ftp-bounce|

invalid-protocol|ip-ttl-zero|ipsproof|land|option-route|router-advt|router-so
licit|

smurf|snork|tcp-bad-sequence|tcp-fin-scan|tcp-intercept|tcp-null-scan|tcp-pos
t-syn|

tcp-sequence-past-window|tcp-xmas-scan|tcphdrfrag|twinge|udp-short-hdr|winnuk
e}
no ip tcp
[adjust-mss|optimize-unnecessary-resends|recreate-flow-on-out-of-state-syn|

validate-icmp-unreachable|validate-rst-ack-number|validate-rst-seq-number]

no ip-mac conflict
no ip-mac routing conflict

no logging [icmp-packet-drop|verbose|malformed-packet-drop]

storm-control [arp|broadcast|multicast|unicast] {fe <1-4>|ge <1-8>|log|
          port-channel <1-8>|up1|wlan <WLAN-NAME>}

no virtual-defragmentation {maximum-fragments-per-datagram|
          minimum-first-fragment-length|maximum-defragmentation-per-host}
```

Parameters

```
no [acl-logging|dhcp-offer-convert|proxy-arp|stateful-packet-inspection-l2]
```

no acl-logging	Disables logging of flow creating traffic
no dhcp-offer-convert	Disables the conversion of broadcast DHCP offers to unicast

no proxy-arp	Disables the generation of ARP responses on behalf of other devices
no stateful-packet-inspection-l2	Disables layer 2 stateful packet inspection

`no alg [dns|ftp|sip|tftp]`

no alg	Disables preconfigured algorithms (dns, ftp, sip, and tftp)
dns	Disables the DNS algorithm
ftp	Disables the FTP algorithm
sip	Disables the SIP algorithm
tftp	Disables the TFTP algorithm

`no clamp tcp-mss`

no clamp tcp-mss	Disables TCP MSS size limiting to the size of the MTU in the inner protocol of a tunneled packet

`no dns-snoop entry-timeout`

no dns	Disables DNS snooping
entry-timeout	Disables DNS snoop table entry timeout

`no firewall enable`

no firewall enable	Disables a device's firewalls

`no flow dhcp stateful`

no flow	Disables firewall flows
dhcp stateful	Disables DHCP stateful flow

`no flow timeout [icmp|other|udp]`

no flow	Disables firewall flow
timeout	Disables the timeout for various packet types
icmp	Disables ICMP packet timeout
others	Disables the timeout for packets other than TCP, ICMP, or UDP
udp	Disables UDP packet timeout

`no flow timeout tcp [closed-wait|established|reset|setup|stateless-fin-or-reset|stateless-general]`

no flow	Disables firewall flows
timeout	Disables the timeout for various packet types
tcp	Disables TCP packet timeout
close-wait	Disables the timeout for TCP flows in close wait status
established	Disables the timeout for TCP flows in established status
reset	Disables the timeout for TCP flows in reset status
setup	Disables the timeout for TCP flows in setup status

stateless-fin-or-reset	Disables the timeout for TCP flows in stateless FIN or RST status
stateless-general	Disables the timeout for TCP flows in general stateless states

`no ip dos {ascend|broadcast-multicast-icmp|chargen|fraggle|ftp-bounce|invalid-protocol|ip-ttl-zero|ipsproof|land|option-route|router-advt|router-solicit|smurf|snork|tcp-bad-sequence|tcp-fin-scan|tcp-intercept|tcp-null-scan|tcp-post-syn|tcp-sequence-past-window|tcp-xmas-scan|tcphdrfrag|twinge|udp-short-hdr|winnuke}`

no ip	Disables IP events
dos	Disables IP DoS events
ascend	Optional. Disables an ASCEND DoS check Ascend routers listen on UDP port 9 for packets from Ascend's Java Configurator. Sending a formatted packet to this port can cause an Ascend router to crash.
broacast-multicast-icmp	Optional. Disables the detection of broadcast or multicast ICMP packets as an attack
chargen	Optional. Disables the chargen service The *Character Generation Protocol* (chargen) is an IP suite service primarily used for testing and debugging networks. It is also used as a generic payload for bandwidth and QoS measurements.
fraggle	Optional. Disables checking for Fraggle DoS attacks. This checks for UDP packets to or from port 7 or 19
ftp-bounce	Optional. Disables FTP bounce attack checks A FTP bounce attack is a MIM attack that enables an attacker to open a port on a different machine using FTP. FTP requires that when a connection is requested by a client on the FTP port (21), another connection must open between the server and the client. To confirm, the PORT command has the client specify an arbitrary destination machine and port for the data connection. This is exploited by the attacker to gain access to a device that may not be the originating client.
invalid-protocol	Optional. Disables a check for invalid protocol number
ip-ttl-zero	Optional. Disables a check for the TCP/IP TTL field with a value of Zero (0)
ipsproof	Optional. Disables IP spoofing DoS attack checks
land	Optional. Disables LAND attack checks *Local Area Network Denial* (LAND) is a DoS attack where IP packets are spoofed and sent to a device where the source IP and destination IP of the packet are the target device's IP, and similarly, the source port and destination port are open ports on the same device. This causes the attacked device to reply to itself continuously.
option-route	Optional. Disables an IP Option Record Route DoS check
router-advt	Optional. Disables router-advt attack checks This is an attack where a default route entry is added remotely to a device. This route entry is given preference, and thereby exposes a vector of attacks.
router-solicit	Optional. Disables router-solicit attack checks Router solicitation messages are sent to locate routers as a form of network scanning. This information can then be used to attack a device.
smurf	Optional. Disables smurf attack checks In this attack, a large number of ICMP echo packets are sent with a spoofed source address. This causes the device with the spoofed source address to be flooded with a large number of replies.

snork	Optional. Disables snork attack checks This attack causes a remote Windows™ NT to consume 100% of the CPU's resources. This attack uses a UDP packtet with a destination port of 135 and a source port of 7, 9, or 135. This attack can also be exploited as a bandwidth consuming attack.
tcp-bad-sequence	Optional. Disables tcp-bad-sequence checks This DoS attack uses a specially crafted TCP packet to cause the targeted device to drop all subsequent network of a specific TCP connection. Disables tcp-bad-sequence check.
tcp-fin-scan	Optional. Disables TCP FIN scan checks A FIN scan finds services on ports. A closed port returns a RST. This allows the attacker to identify open ports
tcp-intercept	Optional. Disables TCP intercept attack checks Prevents TCP intercept attacks by using TCP SYN cookies
tcp-null-scan	Optional. Disables TCP Null scan checks A TCP null scan finds services on ports. A closed port returns a RST. This allows the attacker to identify open ports
tcp-post-syn	Optional. Disables TCP post SYN DoS attack checks
tcp-sequence-past-window	Optional. Disables TCP SEQUENCE PAST WINDOW DoS attack checks Disable this check to work around a bug in Windows XP's TCP stack which sends data past the window when conducting a selective ACK.
tcp-xmas-scan	Optional. Disables TCP XMAS scan checks A TCP XMAS scan finds services on ports. A closed port returns a RST. This allows the attacker to identify open ports
tcphdrfrag	Optional. Disables TCP header checks A DoS attack where the TCP header spans IP fragments
twinge	Optional. Disables twinge attack checks A twinge attack is a flood of false ICMP packets to try and slow down a system
udp-short-hdr	Optional. Disables UDP short header checks Enables the identification of truncated UDP headers and UDP header length fields
winnuke	Optional. Disables Winnuke checks This DoS attack is specific to Windows™ 95 and Windows™ NT, causing devices to crash with a blue screen

```
no ip tcp
[adjust-mss|optimize-unnecessary-resends|recreate-flow-on-out-of-state-syn|va
lidate-icmp-unreachable|validate-rst-ack-number|validate-rst-seq-number]
```

no ip	Disables IP DoS events
tcp	Identifies and disables TCP events and configuration items
adjust-mss	Disables the adjust MSS configuration
optimize-unnecessary-resends	Disables the validation of unnecessary TCP packets
recreate-flow-on-out-of-state-sync	Disallows a TCP SYN packet to delete an old flow in TCP_FIN_FIN_STATE, and TCP_CLOSED_STATE states and create a new flow
validate-icpm-unreachable	Disables the sequence number validation in ICMP unreachable error packets
validate-rst-ack-number	Disables the acknowledgment number validation in RST packets
validate-rst-seq-number	Disables the sequence number validation in RST packets

`no ip-mac conflict`

no ip-mac	Disables IP MAC configuration
conflict	Disables the action performed when a conflict exists between the IP address and MAC address

`no ip-mac routing conflict`

no ip-mac	Disables IP MAC configuration
routing	Configures a routing table based action
conflict	Disables the action performed when a conflict exists in the routing table

`no logging [icmp-packet-drop|verbose|malformed-packet-drop]`

no logging	Disables enhanced firewall logging
icmp-packet-drop	Disables dropping of ICMP packets that do not pass sanity checks
malformed-packet-drop	Disables dropping of raw IP packets that do not pass sanity checks
verbose	Disables verbose logging

`no storm-control [arp|broadcast|multicast|unicast] {fe <1-4>|ge <1-8>|log|port-channel <1-8>|up1|wlan <WLAN-NAME>}`

no storm-control	Disables storm control
arp	Disables storm control for ARP packets
broadcast	Disables storm control for broadcast packets
multicast	Disables storm control for multicast packets
unicast	Disables storm control for unicast packets
fe <1-4>	Disables the FastEthernet port • <1-4> – Sets the FastEthernet port
ge <1-8>	Disables the Gigabit Ethernet port • <1-8> – Sets the GigabitEthernet port
log	Disables storm control logging
port-channel <1-8>	Disables the port channel. • <1-8> – Sets the port channel port
up1	Disables the uplink interface
wlan <WLAN-NAME>	Disables the WLAN • <WLAN-NAME> – Sets the WLAN ID

`no virtual-defragmentation {maximum-fragments-per-datagram|minimum-first-fragment-length|maximum-defragmentation-per-host}`

no virtual-defragmentation	Disables the virtual defragmentation of IPv4 packets
maximum-defragmentation-per-host <1-16384>	Optional. Disables the maximum active IPv4 defragmentation per host
maximum-fragments-per-datagram <2-8129>	Optional. Disables the maximum IPv4 fragments per datagram
minimum-first-fragment-length <8-1500>	Optional. Disables the minimum length required for the first IPv4 fragment

Example

```
rfs7000-37FABE(config-fw-policy-test)#show context
firewall-policy test
 ip dos fraggle drop-only
 no ip dos tcp-sequence-past-window
 ip dos tcp-max-incomplete high 600
 ip dos tcp-max-incomplete low 60
 storm-control broadcast level 20000 ge 4
 storm-control arp log warnings
 ip-mac conflict drop-only
 ip-mac routing conflict log-and-drop log-level notifications
 flow timeout icmp 16000
 flow timeout udp 10000
 flow timeout tcp established 1500
 flow timeout other 16000
 dhcp-offer-convert
 logging icmp-packet-drop rate-limited
 logging malformed-packet-drop all
 logging verbose
 dns-snoop entry-timeout 35
rfs7000-37FABE(config-fw-policy-test)#

rfs7000-37FABE(config-fw-policy-test)#no ip dos fraggle
rfs7000-37FABE(config-fw-policy-test)#no storm-control arp log
rfs7000-37FABE(config-fw-policy-test)#no dhcp-offer-convert
rfs7000-37FABE(config-fw-policy-test)#no logging malformed-packet-drop

rfs7000-37FABE(config-fw-policy-test)#show context
firewall-policy test
 no ip dos fraggle
 no ip dos tcp-sequence-past-window
 ip dos tcp-max-incomplete high 600
 ip dos tcp-max-incomplete low 60
 storm-control broadcast level 20000 ge 4
 storm-control arp log none
 ip-mac conflict drop-only
 ip-mac routing conflict log-and-drop log-level notifications
 flow timeout icmp 16000
 flow timeout udp 10000
 flow timeout tcp established 1500
 flow timeout other 16000
 logging icmp-packet-drop rate-limited
 logging verbose
 dns-snoop entry-timeout 35
rfs7000-37FABE(config-fw-policy-test)#
```

Related Commands:

acl-logging	Enables logging on flow creating traffic
alg	Configures algorithms used with a firewall policy
clamp	Limits the TCP MSS to the MTU value of the inner protocol for tunneled packets
dhcp-offer-convert	Enables the conversion of broadcast DHCP offer packets to unicast
dns-snoop	Configures the DNS snoop table entry timeout
firewall	Enables firewalls

flow	Configures firewall flows
ip	Configures IP settings
ip-mac	Defines actions based on the device IP MAC table
logging	Configures firewall logging
proxy-arp	Enables the generation of ARP responses on behalf of other devices
stateful-packet-inspection-12	Enables layer 2 stateful packet inspection
storm-control	Configures storm control
virtual-defragmentation	Configures the virtual defragmentation of packets at the firewall level

proxy-arp

firewall-policy

Enables the generation of ARP responses on behalf of another device. This option is enabled by default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
proxy-arp
```

Parameters

None

Example

```
rfs7000-37FABE(config-fw-policy-test)#proxy-arp
rfs7000-37FABE(config-fw-policy-test)#
```

Related Commands:

no	Disables the generation of ARP responses on behalf of another device

stateful-packet-inspection-12

firewall-policy

Enables layer 2 firewall stateful packet inspection. This option is enabled by default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
stateful-packet-inspection-l2
```

Parameters

None

Example

```
rfs7000-37FABE(config-fw-policy-test)#stateful-packet-inspection-l2
rfs7000-37FABE(config-fw-policy-test)#
```

Related Commands:

no	Disables stateful packet inspection in a layer 2 firewall

storm-control

firewall-policy

Enables storm control on the firewall policy

Storms are packet bombardments that exceed the high threshold value configured for an interface. During a storm, packets are throttled until the rate falls below the configured rate, severely impacting performance for the RF Domain manager interface.

Storm control limits multicast, unicast and broadcast frames accepted and forwarded by a device. Messages are logged based on their severity level.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
storm-control [arp|broadcast|multicast|unicast]
storm-control [arp|broadcast|multicast|unicast] [level|log]

storm-control [arp|broadcast|multicast|unicast] level <1-1000000> [fe <1-4>|ge
<1-8>|
          port-channel <1-8>|up1|wlan <WLAN-NAME>]

storm-control [arp|broadcast|multicast|unicast] log
[<0-7>|alerts|critical|debugging|
          emergencies|errors|informational|none|notifications|warnings]
```

Parameters

```
storm-control [arp|broadcast|multicast|unicast] level <1-1000000> [fe <1-4>|
ge <1-8>|port-channel <1-8>|up1|wlan <WLAN-NAME>]
```

arp	Configures storm control for ARP packets
broadcast	Configures storm control for broadcast packets
multicast	Configures storm control for multicast packets
unicast	Configures storm control for unicast packets
level <1-1000000>	Configures the allowed number of packets received per second before storm control begins • <1-1000000> – Sets the number of packets received per second
fe <1-4>	Sets the FastEthernet port for storm control from 1 - 4
ge <1-8>	Sets the GigabitEthernet port for storm control from 1 - 8
port-channel <1-8>	Sets the port channel for storm control from 1- 8
up1	Sets the uplink interface
wlan <WLAN-NAME>	Configures the WLAN • <WLAN-NAME> – Sets the WLAN ID for the storm control configuration

```
storm-control [arp|bcast|multicast|unicast] log
[<0-7>|alerts|critical|debugging|
emergencies|errors|informational|none|notifications|warnings]
```

arp	Configures storm control for ARP packets
broadcast	Configures storm control for broadcast packets
multicast	Configures storm control for multicast packets
unicast	Configures storm control for unicast packets
log	Configures the storm control log level for storm control events
<0-7>	Sets the numeric logging level from 0 - 7
alerts	Numerical severity 1. Indicates a condition where immediate action is required
critical	Numerical severity 2. Indicates a critical condition
debugging	Numerical severity 7. Debugging messages
emergencies	Numerical severity 0. System is unusable
errors	Numerical severity 3. Indicates an error condition
informational	Numerical severity 6. Indicates a informational condition
none	Disables storm control logging
notification	Numerical severity 5. Indicates a normal but significant condition
warnings	Numerical severity 4. Indicates a warning condition. This is the default setting.

Example

```
rfs7000-37FABE(config-fw-policy-test)#storm-control arp log warning

rfs7000-37FABE(config-fw-policy-test)#storm-control broadcast level 20000 ge 4

rfs7000-37FABE(config-fw-policy-test)#show context
firewall-policy test
 ip dos fraggle drop-only
 no ip dos tcp-sequence-past-window
 ip dos tcp-max-incomplete high 600
```

```
 ip dos tcp-max-incomplete low 60
 storm-control broadcast level 20000 ge 4
 storm-control arp log warnings
 ip-mac conflict drop-only
 ip-mac routing conflict log-and-drop log-level notifications
 flow timeout icmp 16000
 flow timeout udp 10000
 flow timeout tcp established 1500
 flow timeout other 16000
 dhcp-offer-convert
 logging icmp-packet-drop rate-limited
 logging malformed-packet-drop all
 logging verbose
 dns-snoop entry-timeout 35
rfs7000-37FABE(config-fw-policy-test)#
```

Related Commands:

no	Disables storm control limits on multicast, unicast, and broadcast frames accepted and forwarded by a device

virtual-defragmentation

firewall-policy

Enables the virtual defragmentation of IPv4 packets. This parameter is required for optimal firewall functionality and is enabled by default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
virtual-defragmentation {maximum-defragmentation-per-host <1-16384>|
          maximum-fragments-per-datagram
<2-8129>|minimum-first-fragment-length <8-1500>}
```

Parameters

```
virtual-defragmentation {maximum-defragmentation-per-host <1-16384>|
maximum-fragments-per-datagram <2-8129>|minimum-first-fragment-length
<8-1500>}
```

maximum-defragmentation-per-host <1-16384>	Optional. Defines the maximum active IPv4 defragmentation per host • <1-16384> – Sets a value from 1 - 16384. The default is 8
maximum-fragments-per-datagram <2-8129>	Optional. Defines the maximum IPv4 fragments per datagram (for virtual defragmentation) • <2-8129> – Sets a value from 2 - 8129. The default is 140.
minimum-first-fragment-length <8-1500>	Optional. Defines the minimum length required for the first IPv4 fragment (for virtual defragmentation) • <8-1500> – Sets a value from 8 - 1500 bytes. The default is 8 bytes.

Example

```
rfs7000-37FABE(config-fw-policy-test)#virtual-defragmentation
maximum-fragments-per-datagram 10
rfs7000-37FABE(config-fw-policy-test)#virtual-defragmentation
minimum-first-fragment-length 100
rfs7000-37FABE(config-fw-policy-test)#
```

Related Commands:

no	Resets values or disables virtual defragmentation settings

Chapter

MINT-POLICY 15

This chapter summarizes MiNT policy commands in the CLI command structure.

All communication using the MiNT transport layer can be optionally secured. This includes confidentiality, integrity and authentication of all communications. In addition, a device can be configured to communicate over MiNT with other devices authorized by an administrator.

Use the (config) instance to configure mint-policy related configuration commands. To navigate to the config MiNT policy instance, use the following command:

```
<DEVICE>(config)#mint-policy global-default

rfs7000-37FABE(config-mint-policy-global-default)#?
Mint Policy Mode commands:
  level    Mint routing level
  mtu      Configure the global Mint MTU
  no       Negate a command or set its defaults
  router   Mint router
  udp      Configure mint UDP/IP encapsulation

  clrscr   Clears the display screen
  commit   Commit all changes made in this session
  do       Run commands from Exec mode
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  revert   Revert changes
  service  Service Commands
  show     Show running system information
  write    Write running configuration to memory or terminal

rfs7000-37FABE(config-mint-policy-global-default)#
```

mint-policy

Table 13 summarizes MiNT policy configuration commands.

TABLE 13 MiNT-Policy-Config Commands

Command	Description	Reference
level	Configures the MiNT routing level	page 1010
mtu	Configures the global MiNT MTU	page 1011
no	Negates a command or sets its default	page 1013
router	Configures the priority for MiNT router packets (HELLO, LSP, PSNP, and EXTVLAN)	page 1011
udp	Configures the MiNT UDP/IP encapsulation parameters	page 1012
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386

TABLE 13 MiNT-Policy-Config Commands

Command	Description	Reference
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

level

mint-policy

Configures the global MiNT routing level

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
level 2 area-id <1-16777215>
```

Parameters

```
level 2 area-id <1-16777215>
```

level 2	Configures level 2 inter-site MiNT routing
area-id <1-16777215>	Configures the routing area identifier • <1-16777215> – Specify a value from 1 - 16777215. The level 2 area ID is the global MiNT area identifier. This area identifier separates two overlapping MiNT networks. Configure the level 2 area ID only if there are two MiNT networks sharing the same packet broadcast domain.

Example

```
rfs7000-37FABE(config-mint-policy-global-default)#level 2 area-id 2000

rfs7000-37FABE(config-mint-policy-global-default)#show context
mint-policy global-default
 level 2 area-id 2000
rfs7000-37FABE(config-mint-policy-global-default)#
```

Related Commands:

no	Disables level 2 MiNT packet routing (inter-site packet routing)

mtu

mint-policy

Configures global MiNT *Multiple Transmission Unit* (MTU). Use this command to specify the maximum packet size, in bytes, for MiNT routing. Higher the MTU values, greater is the network efficiency. The user data per packet increases, while protocol overheads, such as headers or underlying per-packet delays remain the same.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
mtu <900-1500>
```

Parameters

```
mtu <900-1500>
```

<900-1500>	Specifies the maximum packet size from 900 - 1500 bytes The maximum packet size specified is rounded down to a value using the following formula: 4 + a multiple of 8. The MTU setting specifies the maximum packet size used for MiNT packets. Larger packets are fragmented to fit within the specified packet size limit. You may want to configure this parameter if the MiNT backhaul network requires or recommends smaller packet sizes. The default value is 1500 bytes.

Example

```
rfs7000-37FABE(config-mint-policy-global-default)#mtu 1000

rfs7000-37FABE(config-mint-policy-global-default)#show context
mint-policy global-default
 mtu 996
 level 2 area-id 2
rfs7000-37FABE(config-mint-policy-global-default)#
```

Related Commands:

no	Reverts the configured MiNT MTU value to its default (1500 bytes) Negates the configured maximum packet size for MiNT routing

router

mint-policy

Configures the priority for MiNT router packets (HELLO, LSP, PSNP, and EXTVLAN)

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
router packet priority <0-7>
```

Parameters

```
router packet priority <0-7>
```

router packet priority <0-7>	Allows you to configure the priority for MiNT router packets from 0 - 7. The default is 5. Higher the value higher is the priority. Therefore, seven (7) represents highest priority.

Example

```
rfs4000-229D58(config-mint-policy-global-default)#router packet priority 4

rfs4000-229D58(config-mint-policy-global-default)#show context
mint-policy global-default
 router packet priority 4
rfs4000-229D58(config-mint-policy-global-default)#
```

Related Commands:

no	Reverts the MiNT router packet priority to default (5)

udp

mint-policy

Configures MiNT UDP/IP encapsulation parameters. Use this command to configure the default UDP port used for MiNT control packet encapsulation.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
udp port <2-65534>
```

Parameters

```
udp port <2-65534>
```

port <2-65534>	Configures default UDP port used for MiNT control packet encapsulation • <2-65534> – Enter a value from 2 - 65534. This value specifies an alternate UDP port used by MiNT control packets and must be an even number. The specified port number plus 1 is used to carry MiNT data packets. The default value is 24576.

Example

```
rfs7000-37FABE(config-mint-policy-global-default)#udp port 1024

rfs7000-37FABE(config-mint-policy-global-default)#show context
mint-policy global-default
 udp port 1024
 mtu 996
 level 2 area-id 2000
 sign-unknown-device
 security-level control-and-data
 rejoin-timeout 1000
rfs7000-37FABE(config-mint-policy-global-default)#
```

Related Commands:

no	Reverts MiNT UDP/IP encapsulation to its default

no

mint-policy

Negates a command or reverts values to their default. When used in the config MiNT policy mode, the no command resets or reverts the following global MiNT policy parameters: routing level, MTU, router packet priority, and UDP or IP encapsulation settings.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no [level|mtu|router|udp]

no level 2 area-id

no mtu

no router packet priority

no udp port <LINE-SINK>
```

Parameters

`no level 2 area-id`

no level 2	Disables level 2 MiNT routing
area identifier	Negates the area identifier

`no mtu`

no mtu	Reverts the configured MiNT MTU value to its default

`no router packet priority`

no router packet priority	Resets the MiNT router packet priority to default

`no udp port <LINE-SINK>`

no udp	Resets the UDP/IP encapsulation parameters to its default
port <LINE-SINK>	Uses the default UDP port for MiNT encapsulation

Example

The following example shows the global Mint Policy parameters before the **'no'** commands are executed:

```
rfs7000-37FABE(config-mint-policy-global-default)#show context
mint-policy global-default
 udp port 1024
 mtu 996
 level 2 area-id 2000
 sign-unknown-device
 security-level control-and-data
 rejoin-timeout 1000
rfs7000-37FABE(config-mint-policy-global-default)#

rfs7000-37FABE(config-mint-policy-global-default)#no level 2 area-id
rfs7000-37FABE(config-mint-policy-global-default)#no mtu
rfs7000-37FABE(config-mint-policy-global-default)#no udp port
```

The following example shows the global Mint Policy parameters after the **'no'** commands are executed:

```
rfs7000-37FABE(config-mint-policy-global-default)#show context
mint-policy global-default
 sign-unknown-device
 security-level control-and-data
 rejoin-timeout 1000
rfs7000-37FABE(config-mint-policy-global-default)#
```

Related Commands:

level	Configures the global MiNT routing level
mtu	Configures the global MiNT MTU
router	Configures the priority for MiNT router packets (HELLO, LSP, PSNP, and EXTVLAN)
udp	Configures the MiNT UDP/IP encapsulation parameters

Chapter

MANAGEMENT-POLICY 16

This chapter summarizes management policy commands in the CLI command structure.

A management policy contains configuration elements for managing a device, such as access control, SNMP, admin user credentials, and roles.

A controller (wireless controller, access point, or service platform) uses mechanisms to allow or deny device access to separate interfaces and protocols (*HTTP, HTTPS*, *Telnet*, *SSH* or *SNMP*). Management access can be enabled or disabled as required for unique policies. The management access functionality is not meant to function as an ACL (in routers or other firewalls), where administrators specify and customize specific IPs to access specific interfaces.

Controllers and service platforms can be managed using multiple interfaces (SNMP, CLI and Web UI). By default, management access is unrestricted, allowing management access to any enabled IP interface from any host using any enabled management service.

To enhance security, administrators can do the following:

- Restrict SNMP, CLI and Web UI access to specific hosts or subnets
- Disable un-used and insecure interfaces as required within managed access profiles. Disabling un-used management services can dramatically reduce an attack footprint and free resources on managed devices
- Provide authentication for management users
- Apply access restrictions and permissions to management users

  Management restrictions can be applied to meet specific policies or industry requirements requiring only certain devices or users be granted access to critical infrastructure devices. Management restrictions can also be applied to reduce the attack footprint of the device when guest services are deployed.

  Access Points utilize a single management access policy, so ensure all the intended administrative roles, permissions, authentication and SNMP settings are correctly set. If an access point is functioning as a virtual controller AP, these are the access settings used by adopted access points of the same model as the virtual controller AP.

Brocade recommends disabling un-used and insecure interfaces as required within managed access profiles. Disabling un-used management services can dramatically reduce an attack footprint and free resources on managed devices.

Use the (config) instance to configure a management policy. To navigate to the config management policy instance, use the following commands:

```
<DEVICE>(config)#management-policy <POLICY-NAME>

rfs7000-37FABE(config)#management-policy test
```

To commit a management-policy, at least one admin user account must always be present in the management-policy:

```
rfs7000-37FABE(config-management-policy-test)#user admin password 0
motorolasolutions role superuser access all
rfs7000-37FABE(config-management-policy-test)#
```

```
rfs7000-37FABE(config-management-policy-test)#?
Management Mode commands:
  aaa-login                Set authentication for logins
  banner                   Define a login banner
  ftp                      Enable FTP server
  http                     Hyper Text Terminal Protocol (HTTP)
  https                    Secure HTTP
  idle-session-timeout     Configure idle timeout for a configuration session
                           (GUI or CLI)
  no                       Negate a command or set its defaults
  privilege-mode-password  Set the password for entering CLI privilege mode
  restrict-access          Restrict management access to the device
  snmp-server              SNMP
  ssh                      Enable ssh
  telnet                   Enable telnet
  user                     Add a user account

  clrscr                   Clears the display screen
  commit                   Commit all changes made in this session
  do                       Run commands from Exec mode
  end                      End current mode and change to EXEC mode
  exit                     End current mode and down to previous mode
  help                     Description of the interactive help system
  revert                   Revert changes
  service                  Service Commands
  show                     Show running system information
  write                    Write running configuration to memory or terminal

rfs7000-37FABE(config-management-policy-test)#
```

management-policy

Table 14 summarizes management policy configuration commands.

TABLE 14 Management-Policy-Config Commands

Command	Description	Reference
aaa-login	Configures login authentication settings	page 1017
banner	Configures the *message of the day* (motd) text	page 1018
ftp	Enables FTP on this management policy	page 1019
http	Enables HTTP on this management policy	page 1021
https	Enables HTTPS on this management policy	page 1021
idle-session-timeout	Sets the interval after which an idle session is terminated	page 1022
no	Removes or resets this management policy's settings	page 1023
privilege-mode-password	Configures the CLI's privilege mode access password	page 1026
restrict-access	Restricts management access to a set of hosts or subnets	page 1027
snmp-server	Sets the SNMP server settings on this management policy	page 1029
ssh	Enables SSH on this management policy	page 1033
telnet	Enables Telnet on this management policy	page 1034

TABLE 14 Management-Policy-Config Commands

Command	Description	Reference
user	Creates a new user account	page 1035
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 1037
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
show	Displays running system information	page 429

aaa-login

management-policy

Configures *Authentication, Authorization and Accounting* (AAA) authentication mode used with this management policy. The different modes are: local authentication and external RADIUS server authentication.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
aaa-login [local|radius|tacacs]

aaa-login local

aaa-login radius [external|fallback|policy]
aaa-login radius [external|fallback|policy <AAA-POLICY-NAME>]

aaa-login tacacs [accounting|authentication|authorization|fallback|policy]
aaa-login tacacs [accounting|authentication|authorization|fallback|
          policy <AAA-TACACS-POLICY-NAME>]
```

Parameters

`aaa-login local`

local	Sets local as the preferred authentication mode. Local authentication uses the local username database to authenticate a user.

`aaa-login radius [external|fallback|policy <AAA-POLICY-NAME>]`

radius	Configures the RADIUS server parameters If local authentication is disabled, use this command to specify if the RADIUS server used is external, fallback, or specified by a AAA policy.
external	Configures external RADIUS server as the preferred authentication mode
fallback	Configures RADIUS server authentication as the primary authentication mode. When RADIUS server authentication fails, the system uses local authentication. This command configures local authentication as a backup mode.
policy <AAA-POLICY-NAME>	Associates a specified AAA policy with this management policy. The AAA policy determines if a client is granted access to the network. • <AAA-POLICY-NAME> – Specify the AAA policy name (should be existing and configured). For more information on configuring AAA policy, see *AAA-POLICY*.

`aaa-login tacacs [accounting|authentication|authorization|fallback| policy <AAA-TACACS-POLICY-NAME>]`

tacacs	Configures *Terminal Access Control Access-Control System* (TACACS) server parameters
accounting	Configures TACACS accounting
authentication	Configures TACACS authentication
authorization	Configures TACACS authorization
fallback	Configures TACACS as the primary authentication mode. When TACACS authentication fails, the system uses local authentication. This command configures local authentication as a backup mode.
policy <AAA-TACACS-POLICY-NAME>	Associates a specified AAA TACACS policy with this management policy • <AAA-TACACS-POLICY-NAME> – Specify the TACACS policy name (should be existing and configured). For more information on configuring AAA TACACS policy, see *AAA-TACACS-POLICY*.

Usage Guidelines:

Use AAA login to determine whether management user authentication must be performed against a local user database or an external RADIUS server.

Example

```
rfs7000-37FABE(config-management-policy-test)#aaa-login radius external

rfs7000-37FABE(config-management-policy-test)#aaa-login radius policy test

rfs7000-37FABE(config-management-policy-test)#show context
management-policy test
 http server
 no ssh
 aaa-login radius external
 aaa-login radius policy test
rfs7000-37FABE(config-management-policy-test)#
```

Related Commands:

no	Removes the TACACS server settings

banner

management-policy

Configures the *message of the day* (motd) text. This text is displayed at login to clients connecting through Telnet or SSH.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
banner motd <LINE>
```

Parameters

```
banner motd <LINE>
```

motd <LINE>	Sets the motd banner • <LINE> – Enter the message string. The message string should not exceed 255 characters.

Example

```
rfs7000-37FABE(config-management-policy-test)#banner motd “Have a Good Day”

rfs7000-37FABE(config-management-policy-test)#show context
management-policy test
 http server
 no ssh
 aaa-login radius external
 aaa-login radius policy test
 banner motd “Have a Good Day”
rfs7000-37FABE(config-management-policy-test)#
```

Related Commands:

no	Removes the motd banner

ftp

management-policy

Enables *File Transfer Protocol* (FTP) on this management policy. FTP is the standard protocol for transferring files over a TCP/IP network. FTP requires administrators enter a valid username and password authenticated locally. FTP access is disabled by default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
ftp {password|rootdir|username}

ftp {password [1 <ENCRYPTED-PASSWORD>|<PASSWORD>]}

ftp {rootdir <DIR>}

ftp {username <USERNAME> password [1 <ENCRYPTED-PASSWORD>|<PASSWORD>] rootdir
<DIR>}
```

Parameters

`ftp {password [1 <ENCRYPTED-PASSWORD>|<PASSWORD>]}`

ftp password	Optional. Configures the FTP server password
1 <ENCRYPTED-PASSWORD>	Configures an encrypted password. Use this option when copy pasting the password from another device. • <ENCRYPTED-PASSWORD> – Specify the password. The password should not exceed 63 characters in length.
<PASSWORD>	Configures a clear text password

`ftp {rootdir <DIR>}`

ftp rootdir <DIR>	Optional. Configures the root directory for FTP logins • <DIR> – Specify the root directory path. By default the root directory is set to flash:/

`ftp {username <USERNAME> password [1 <ENCRYPTED-PASSWORD>|<PASSWORD>] rootdir <DIR>}`

ftp username <USERNAME>	Optional. Configures a new user account on the FTP server. The FTP user file lists users with FTP server access. • <USERNAME> – Specify the username. The username should not exceed 32 characters in length.
password 1 [<ENCRYPTED-PASSWORD> | <PASSWORD>]	Configures an encrypted password • <ENCRYPTED-PASSWORD> – Specifies an encrypted password (use this option if copy pasting from another device). The password should not exceed 63 characters in length. • <PASSWORD> – Configures a clear text password
rootdir <DIR>	After specifying the password, configure the FTP root directory. • rootdir <DIR> – Configures the root directory for FTP logins. Specify the root directory path.

Usage Guidelines:

The string size of an encrypted password (option 1, password is encrypted with a SHA1 algorithm) must be exactly 40 characters.

Example

```
rfs7000-37FABE(config-management-policy-test)#ftp username superuser password
motorolasolutions@123 rootdir dir

rfs7000-37FABE(config-management-policy-test)#show context
management-policy test
 http server
 ftp username superuser password 1
7ccb4568cb83e54f1e402f785a78ee930a453afda152baaf7c2b79277f225872 rootdir dir
 no ssh
 aaa-login radius external
 aaa-login radius policy test
 banner motd "Have a Good Day"
rfs7000-37FABE(config-management-policy-test)#
```

Related Commands:

no	Disables FTP and its settings, such as the server password, root directory, and users

http

management-policy

Enables *Hyper Text Transport Protocol* (HTTP) on this management policy

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
http server
```

Parameters

```
http server
```

http server	Enables HTTP on this management policy. HTTP provides limited authentication and no encryption.

Example

```
rfs7000-37FABE(config-management-policy-test)#http server

rfs7000-37FABE(config-management-policy-test)#show context
management-policy test
 http server
 ftp username superuser password 1
7ccb4568cb83e54f1e402f785a78ee930a453afda152baaf7c2b79277f225872 rootdir dir
 no ssh
 aaa-login radius external
 aaa-login radius policy test
 banner motd "Have a Good Day"
rfs7000-37FABE(config-management-policy-test)#
```

Related Commands:

no	Disables HTTP on this management policy

https

management-policy

Enables *Hyper Text Transport Protocol Secure* (HTTPS) on this management policy

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
https server
```

Parameters

```
https server
```

https server	Enables HTTPS on this management policy. HTTPS provides both authentication and data encryption as opposed to just authentication.

Example

```
rfs7000-37FABE(config-management-policy-test)#https server

rfs7000-37FABE(config-management-policy-test)#show context
management-policy test
 http server
 https server
 ftp username superuser password 1
7ccb4568cb83e54f1e402f785a78ee930a453afda152baaf7c2b79277f225872 rootdir dir
 no ssh
 aaa-login radius external
 aaa-login radius policy test
 banner motd "Have a Good Day"
rfs7000-37FABE(config-management-policy-test)#
```

Related Commands:

no	Disables HTTPS on this management policy

idle-session-timeout

management-policy

Configures a session's idle timeout. An idle session is automatically terminated after the specified interval is exceeded.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
idle-session-timeout <1-4320>
```

Parameters

```
idle-session-timeout <1-4320>
```

<1-4320>	Sets the interval, in minutes, after which an idle session is timed out. Specify a value from 1 - 4320 minutes. The default is 30 minutes.

Example

```
rfs7000-37FABE(config-management-policy-test)#idle-session-timeout 100

rfs7000-37FABE(config-management-policy-test)#show context
management-policy test
 http server
 https server
 ftp username superuser password 1
7ccb4568cb83e54f1e402f785a78ee930a453afda152baaf7c2b79277f225872 rootdir dir
 no ssh
 aaa-login radius external
 aaa-login radius policy test
 idle-session-timeout 100
 banner motd "Have a Good Day"
rfs7000-37FABE(config-management-policy-test)#
```

Related Commands:

no	Removes the configured idle session timeout value

no

management-policy

Negates a command or reverts values to their default. When used in the config management policy mode, the no command negates or reverts management policy settings.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no
[aaa-login|banner|ftp|http|https|idle-session-timeout|privilege-mode-password
|
          restrict-access|snmp-server|ssh|telnet|user|service]

no aaa-login tacacs [accounting|authentication|authorization|fallback|policy]

no banner motd

no ftp {password|rootdir}

no [http|https] server
```

```
no [idle-session-timeout|privilege-mode-password|restrict-access]

no snmp-server [community|display-vlan-info-per-radio|enable|host|manager|

max-pending-requests|request-timeout|suppress-security-configuration-level|
          throttle|user]

no snmp-server [community <WORD>|display-vlan-info-per-radio|enable traps|
          host <IP> {<1-65535>}|manager
[all|v1|v2|v3]|max-pending-requests|request-timeout|
          suppress-security-configuration-level|throttle|user
[snmpmanager|snmpoperator|
          snmptrap]]

no ssh {login-grace-time|port|use-key}

no [telnet|user <USERNAME>]

no service prompt crash-info
```

Parameters

`no aaa-login tacacs [accounting|authentication|authorization|fallback|policy]`

no aaa-login	Disables or reverts user authorization parameters
tacacs	Disables the TACACS server parameters
accounting	Disables TACACS accounting
authentication	Disables TACACS authentication
authorization	Disables TACACS authorization
fallback	Disables TACACS as the primary authentication mode
policy	Disassociates a specified TACACS policy from this management policy

`no banner motd`

no banner motd	Removes the motd banner

`no ftp {password|rootdir}`

no ftp	Reverts to default FTP server settings
password	Optional. Reverts to default FTP password
rootdir	Optional. Reverts to default FTP root directory

`no [http|https] server`

no http	Disables the HTTP server on this management policy
no https	Disables the HTTPS server on this management policy

`no [idle-session-timeout|privilege-mode-password|restrict-access]`

no idle-session-timeout	Disables a defined session timeout interval
no privilege-mode-password	Removes the configured CLI privilege mode access password
no restrict-session	Removes management access restrictions on this management policy

```
no snmp-server [community <WORD>|display-vlan-info-per-radio|enable traps|host
<IP> {<1-65535>}|manager [all|v1|v2|v3]|max-pending-requests|request-timeout|
suppress-security-configuration-level|throttle|user
[snmpmanager|snmpoperator|
snmptrap]]
```

no snmp-server	Disables the SNMP server parameters
community <WORD>	Disables SNMP server access to a community • <WORD> – Specify the community name.
display-vlan-info-per-radio	Disables the display of the VLAN ID along with the radio interface ID (only displays the radio interface)
enable traps	Disables SNMP traps
host <IP> {<1-65535>}	Removes SNMP host (trap recipient) details • <IP> – Specify the host's IP address. • <1-65535> – Optional. Resets the port for receiving SNMP traps to default (162)
manager [all|v1|v2|v3]	Disables SNMP manager
max-pending-requests	Resets the maximum pending requests to default (128)
request-timeout	Resets the request timeout to default (240 seconds)
suppress-security-configuration-level	Reverts the SNMP security configuration suppression level to default (Level 0)
throttle	Disables CPU throttle for SNMP
user [snmpmanager|snmpoperator|snmptrap]	Removes a SNMPv3 user from this management policy • snmpmanager – Removes a SNMP manager account • snmpoperator – Removes a SNMP operator account • snmptrap – Removes a SNMP trap user account

```
no ssh {login-grace-time|port|use-key}
```

no ssh {login-grace-time|port|use-key}	Resets the following secure shell settings: • login-grace-time – Optional. Resets SSH login grace time to its default (60 seconds) • port – Optional. Resets SSH port to default (port 22) • use-key – Optional. Resets RSA key to default

```
no [telnet|user <USERNAME>]
```

no telnet	Disables Telnet on this management policy
no user <USERNAME>	Removes a specified user account from this management policy • <USERNAME> – Specify the account's username.

```
no service prompt crash-info
```

no service	Disables service commands
prompt	Disables the updating of CLI prompt settings
crash-info	Excludes asterisks (*) at the end of the prompt, if the device has crash files in flash:/crashinfo

Example

```
The following example shows the management policy 'test' settings before the
'no' commands are executed:

rfs7000-37FABE(config-management-policy-test)#show context
management-policy test
 http server
 https server
```

```
 ftp username superuser password 1
7ccb4568cb83e54f1e402f785a78ee930a453afda152baaf7c2b79277f225872 rootdir dir
 no ssh
 aaa-login radius external
 aaa-login radius policy test
 idle-session-timeout 100
 banner motd "Have a Good Day"
rfs7000-37FABE(config-management-policy-test)#

rfs7000-37FABE(config-management-policy-test)#no banner motd
rfs7000-37FABE(config-management-policy-test)#no idle-session-timeout
rfs7000-37FABE(config-management-policy-test)#no http server

The following example shows the management policy ‘test’ settings after the
‘no’ commands are executed:

rfs7000-37FABE(config-management-policy-test)#show context
management-policy test
 no http server
 https server
 ftp username superuser password 1
626b4033263d6d2ae4e79c48cdfcccb60fd4c77a8da9e365060597a6d6570ec2 rootdir dir
 no ssh
 aaa-login radius external
 aaa-login radius policy test
 idle-session-timeout 0
rfs7000-37FABE(config-management-policy-test)#
```

Related Commands:

aaa-login	Configures the AAA authentication mode used with this management policy
banner	Configures the login motd banner
ftp	Configures the FTP server parameters
http	Enables HTTP
https	Enables HTTPS
idle-session-timeout	Configures a session’s idle timeout
privilege-mode-password	Configures the CLI’s privilege mode access password
restrict-access	Restricts management access to a set of hosts or subnets. Also enables the logging of access requests
snmp-server	Configures SNMP engine parameters
ssh	Enables a SSH connection between client and server
telnet	Enables Telnet
user	Adds a new user account
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations

privilege-mode-password

management-policy

Configures the CLI’s privilege mode access password

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
privilege-mode-password [1 <PASSWORD>|<PASSWORD>]
```

Parameters

```
privilege-mode-password [1 <PASSWORD>|<PASSWORD>]
```

1 <PASSWORD>	Configures an encrypted password. Use this option when copy pasting the password from another device. • <PASSWORD> – Enter the password.
<PASSWORD>	Configures a clear text password • <PASSWORD> – Enter the password.

Example

```
rfs7000-37FABE(config-management-policy-test)#privilege-mode-password
testing@1234
rfs7000-37FABE(config-management-policy-test)#

rfs7000-37FABE(config-management-policy-test)#show context
management-policy test
 http server
 no ssh
 privilege-mode-password 1
2e9f038ac2ed27f919ed5a4dceb3d30e32f356f2ceff6fbf26a153d0339c
734f
rfs7000-37FABE(config-management-policy-test)#
```

Related Commands:

no	Removes the configured CLI privilege mode access password

restrict-access

management-policy

Restricts management access to a set of hosts or subnets

Restricting remote access to a controller or service platform ensures only trusted hosts can communicate with enabled management services. This ensures only trusted hosts can perform management tasks and provide protection from brute force attacks from hosts attempting to break into the controller or service platform managed network.

Administrators can permit management connections to be established on any IP interface on the controller or service platform (including IP interfaces used to provide captive portal guest access). Administrators can restrict management access by limiting access to a specific host (IP address), subnet, or ACL on the controller or service platform.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
restrict-access [host|ip-access-list|subnet]

restrict-access host <IP> {<IP>|log|subnet}
restrict-access host <IP> {<IP>|log [all|denied-only]}
restrict-access host <IP> {subnet <IP/M> {<IP/M>|log [all|denied-only]}}

restrict-access ip-access-list <IP-ACCESS-LIST-NAME>

restrict-access subnet <IP/M> {<IP/M>|host|log}
restrict-access subnet <IP/M> {<IP/M>|log [all|denied-only]}
restrict-access subnet <IP/M> {host <IP> {log [all|denied-only]}}
```

Parameters

```
restrict-access host <IP> {<IP>|log [all|denied-only]}
```

host <IP>	Restricts management access to a specified host. Filters access requests based on a host's IP address • <IP> – Specify the host's IP address.
<IP>	Optional. Use this option to add multiple hosts, if required, to the restrict access list.
log [all|denied-only]	Optional. Configures a logging policy for access requests. Sets the log type generated for access requests • all – Logs all access requests, both denied and permitted • denied-only – Logs only denied access (when an access request is received from a host denied access, a record is logged)

```
restrict-access host <IP> {subnet <IP/M> {<IP/M>|log [all|denied-only]}}
```

host <IP>	Restricts management access to a specified host. Uses the IP address of a host to filter access requests • <IP> – Specify the host's IP address.
subnet <IP/M>	Optional. Restricts access to the host on a specified subnet. Uses a subnet IP address as a second filter option • <IP/M> – Sets the subnet IP address in the A.B.C.D/M format
<IP/M>	Optional. Use this option to add multiple subnets, if required, to the restrict access list.
log [all|denied-only]	Optional. Configures a logging policy for access requests. Sets the log type generated for access requests • all – Logs all access requests, both denied and permitted • denied-only – Logs only denied access (when an access request is received from a host denied access, a record is logged)

```
restrict-access ip-access-list <IP-ACCESS-LIST-NAME>
```

ip-access-list	Uses an IP access list to filter access requests IP based firewalls function like *Access Control Lists* (ACLs) to filter/mark packets based on the IP from which they arrive, as opposed to filtering packets on layer 2 ports. IP firewalls implement uniquely defined access control policies. To have effective firewalls, you need to have a clear idea of the kind of access to allow or deny. A poorly defined firewall is of little value, and could provide a false sense of network security.
<IP-ACCESS-LIST-NAME>	Sets the access list name

`restrict-access subnet <IP/M> {<IP/M>|log [all|denied-only]}`

subnet <IP/M>	Restricts access to a specified subnet. Uses a subnet IP address to filter access requests • <IP/M> – Sets the IP address of the subnet in the A.B.C.D/M format
<IP/M>	Optional. Use this option to add multiple subnets, if required, to the restrict access list.
log [all|denied-only]	Optional. Configures a logging policy for access requests. Sets the log type generated for access requests • all – Logs all access requests, both denied and permitted • denied-only – Logs only denied access (when an access request is received from a host denied access, a record is logged)

`restrict-access subnet <IP/M> {host <IP> {log [all|denied-only]}}`

subnet <IP/M>	Restricts access to a specified subnet. Uses a subnet IP address to filter access requests • <IP/M> – Sets the IP address of the subnet in the A.B.C.D/M format
host <IP>	Uses the host IP address as a second filter • <IP> – Specify the host IP address.
log [all|denied-only]	Optional. Configures a logging policy for access requests. Sets the log type generated for access requests • all – Logs all access requests, both denied and permitted • denied-only – Logs only denied access (when an access request is received from a host denied access, a record is logged)

Example

```
rfs7000-37FABE(config-management-policy-test)#restrict-access host
172.16.10.4 log denied-only

rfs7000-37FABE(config-management-policy-test)#show context
management-policy test
 no http server
 https server
 ftp username superuser password 1
626b4033263d6d2ae4e79c48cdfcccb60fd4c77a8da9e365060597a6d6570ec2 rootdir dir
 no ssh
 aaa-login radius external
 aaa-login radius policy test
 idle-session-timeout 0
 restrict-access host 172.16.10.4 log denied-only
rfs7000-37FABE(config-management-policy-test)#
```

Related Commands:

no	Removes device access restrictions

snmp-server

management-policy

Enables the *Simple Network Management Protocol* (SNMP) engine settings. SNMP is an application layer protocol that facilitates the exchange of management information between the controller and a managed device. SNMP enabled devices listen on port 162 (by default) for SNMP packets from the controller's management server. SNMP uses read-only and read-write community strings as an authentication mechanism to monitor and configure supported devices. The read-only community string gathers statistics and configuration parameters from a supported wireless device. The read-write community string is used by a management server to *set* device parameters. SNMP is generally used to monitor a system's performance and other parameters.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
snmp-server [community|enable|display-vlan-info-per-radio|host|manager|

max-pending-requests|request-timeout|suppress-security-configuration-level|
          throttle|user]

snmp-server community [0 <WORD>|2 <WORD>|<WORD>] [ro|rw]

snmp-server enable traps

snmp-server host <IP> [v2c|v3] {<1-65535>}

snmp-server manager [all|v1|v2|v3]

snmp-server [max-pending-requests {<64-1024>}|request-timeout {<2-720>}]

snmp-server [display-vlan-info-per-radio|throttle <1-100>|
          suppress-security-configuration-level [0|1]]

snmp-server user [snmpmanager|snmpoperator|snmptrap]
snmp-server user [snmpmanager|snmpoperator|snmptrap] v3 [auth|encrypted]

snmp-server user [snmpmanager|snmpoperator|snmptrap] v3 auth md5
          [0 <PASSWORD>|2 <ENCRYPTED-PASSWORD>|<PASSWORD>]

snmp-server user [snmpmanager|snmpoperator|snmptrap] v3 encrypted
          [auth md5|des auth md5] [0 <PASSWORD>|2 <ENCRYPTED-PASSWORD>|
<PASSWORD>]
```

Parameters

```
snmp-server community [0 <WORD>|2 <WORD>|<WORD>] [ro|rw]
```

community [0 <WORD>|2 <WORD>|<WORD>]	Sets the community string and associated access privileges. Enables SNMP access by configuring community strings that act like passwords. Configure different types of community strings, each string providing a different form of access. Provide either *read-only* (ro) or *read-write* (rw) access. • 0 <WORD> – Sets a clear text SNMP community string • 2 <WORD> – Sets an encrypted SNMP community string • <WORD> – Sets the SNMP community string
[ro|rw]	After configuring the SNMP community string, assign one of the following accesses: • ro – Assigns read-only access to the specified SNMP community (allows a remote device to retrieve information) rw – Assigns read and write access to the specified SNMP community (allows a remote device to modify settings)

	`snmp-server enable traps`
enable traps	Enables trap generation (using the trap receiver configuration defined). This feature is disabled by default. Enabling this feature ensures the dispatch of SNMP notifications to all hosts. In a managed network, the controller uses SNMP trap receivers to notify faults. SNMP traps are unsolicited notifications triggered by thresholds (or actions) on devices and are therefore an important fault management tool. A SNMP trap receiver is the destination of SNMP messages (external to the controller). A trap is like a Syslog message, just over another protocol (SNMP). A trap is generated when a device consolidates event information and transmits the information to an external repository. The trap contains several standard items, such as the SNMP version, community etc. SNMP trap notifications exist for most controller operations, but not all are necessary for day-to-day operation.
	`snmp-server host <IP> [v2c|v3] {<1-65535>}`
host <IP>	Configures a host's IP address. This is the external server resource dedicated to receiving SNMP traps on behalf of the controller.
[v2c|v3]	Configures the SNMP version used to send the traps • v2c – Uses SNMP version 2c • v3 – Uses SNMP version 3
<1-65535>	Optional. Specifies the host's UDP port number. This is port used by the external resource to receive SNMP traps. <1-65535> – Optional. Sets a value from 1 - 65535. The default port is 162.
	`snmp-server manager [all|v1|v2|v3]`
manager [all|v2|v3]	Enables SNMP manager and specifies the SNMP version • all – Enables SNMP manager version v2 and v3 • v1 – Enables SNMP manager version v1 only. SNMPv1 uses a simple password ("community string"). Data is unencrypted (clear text). Consequently it provides limited security, and should be used only inside LANs behind firewalls, not in WANs. • v2 – Enables SNMP manager version v2 only. SNMPv2 provides device management using a hierarchical set of variables. SNMPv2 uses *Get*, *GetNext*, and *Set* operations for data management. SNMPv2 is enabled by default. • v3 – Enables SNMP manager version v3 only. SNMPv3 adds security and remote configuration capabilities to previous versions. The SNMPv3 architecture introduces the *User-based Security Model* (USM) for message security and the *View-based Access Control Model* (VACM) for access control. The architecture supports the concurrent use of different security, access control and message processing techniques. SNMPv3 is enabled by default.
	`snmp-server [max-pending-requests {<64-1024>}|request-timeout {<2-720>}]`
max-pending-requests {<64-1024>}	Sets the maximum number of requests that can be pending at any given time • <64-1024> – Optional. Specify a value from 64 - 1024. The default is 128.
request-timeout {<2-720>}	Sets the interval, in seconds, after which an error message is returned for a pending request • <2-720> – Optional. Specify a value from 2 - 720 seconds. The default is 240 seconds.
	`snmp-server [display-vlan-info-per-radio|throttle <1-100>| suppress-security-configuration-level [0|1]]`
display-vlan-info-per-radio	Enables the display of the VLAN ID along with the radio interface ID

throttle <1-100>	Sets CPU usage for SNMP activities. Use this command to set the CPU usage from 1 - 100.

suppress-security-configuration-level [0|1]	Sets the level of suppression of SNMP security configuration information
	• 0 – If this option is selected, an empty string is returned for the SNMP request for security configuration information. Security configuration information consists of:
	  • Passwords
	  • Keys
	  • Shared secrets
	The default setting is 0.
	• 1 – Suppresses the display of the policy, IP ACL, passwords, keys and shared secrets. If this option is selected, in addition to suppression from 'Level 0', an empty string is returned for a SNMP request on following items:
	  • Management policies
	  • IP ACL
	  • Tables containing user names and community strings

`snmp-server user [snmpmanager|snmpoperator|snmptrap] v3 auth md5 [0 <PASSWORD>|2 <ENCRYPTED-PASSWORD>|<PASSWORD>]`

user [snmpmanager| snmpoperator| snmptrap]	Defines user access to the SNMP engine • snmpmanager – Sets user as a SNMP manager • snmpoperator – Sets user as a SNMP operator • snmptrap – Sets user as a SNMP trap user
v3 auth md5	Uses SNMP version 3 as the security model • auth – Uses an authentication protocol • md5 – Uses HMAC-MD5 algorithm for authentication
[0 <PASSWORD>| 2 <ENCRYPTED-PASSWORD>| <PASSWORD>]	Configures password using one of the following options: • 0 <PASSWORD> – Configures clear text password • 2 <PASSWORD> – Configures encrypted password • <PASSWORD> – Specifies a password for authentication and privacy protocols

`snmp-server user [snmpmanager|snmpoperator|snmptrap] v3 encrypted [auth md5|des auth md5] [0 <PASSWORD>|2 <ENCRYPTED-PASSWORD>|<PASSWORD>]`

user [snmpmanager| snmpoperator| snmptrap]	Defines user access to the SNMP engine • snmpmanager – Sets user as a SNMP manager • snmpoperator – Sets user as a SNMP operator • snmptrap – Sets user as a SNMP trap user
v3 encrypted	Uses SNMP version 3 as the security model • encrypted – Uses encrypted privacy protocol
auth md5	Uses authentication protocol • auth – Sets authentication parameters • md5 – Uses HMAC-MD5 algorithm for authentication

des auth md5	Uses privacy protocol for user privacy
	• des – Uses CBC-DES for privacy
	After specifying the privacy protocol, specify the authentication mode.
	  • auth – Sets user authentication parameters
	  • md5 – Uses HMAC-MD5 algorithm for authentication

[0 <PASSWORD>| 2 <ENCRYPTED-PASSWORD>| <PASSWORD>]	The following are common to both the auth and des parameters: Configures password using one of the following options: • 0 <PASSWORD> – Configures a clear text password • 2 <PASSWORD> – Configures an encrypted password • <PASSWORD> – Specifies a password for authentication and privacy protocols

Example

```
rfs7000-37FABE(config-management-policy-test)#snmp-server community snmp1 ro

rfs7000-37FABE(config-management-policy-test)#snmp-server host 172.16.10.23
v3 162

rfs7000-37FABE(config-management-policy-test)#commit

rfs7000-37FABE(config-management-policy-test)#snmp-server user snmpmanager v3
auth md5 motorola1123

rfs7000-37FABE(config-management-policy-test)#show context
management-policy test
 no http server
 https server
 ftp username superuser password 1
626b4033263d6d2ae4e79c48cdfcccb60fd4c77a8da9e365060597a6d6570ec2 rootdir dir
 no ssh
 snmp-server community snmp1 ro
 snmp-server user snmpmanager v3 encrypted des auth md5 0 motorola1123
 snmp-server host 172.16.10.23 v3 162
 aaa-login radius external
 aaa-login radius policy test
 idle-session-timeout 0
 restrict-access host 172.16.10.2 log all
rfs7000-37FABE(config-management-policy-test)#
```

Related Commands:

no	Disables or resets the SNMP server settings

ssh

management-policy

Enables *Secure Shell* (SSH) for this management policy

SSH, like Telnet, provides a command line interface to a remote host. SSH transmissions are encrypted and authenticated, increasing the security of transmission. SSH access is disabled by default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
ssh {login-grace-time <60-300>|port <1-65535>}
```

Parameters

```
ssh {login-grace-time <60-300>|port <1-65535>}
```

ssh	Enables SSH communication between client and server
login-grace-time <60-300>	Optional. Configures the login grace time. This is the interval, in seconds, after which an unsuccessful login is disconnected. • <60-300> – Specify a value from 60 - 300 seconds. The default is 60 seconds.
port <1-65535>	Optional. Configures the SSH port. This is the port used for SSH connections. • <1-65535> – Specify a value from 1 - 165535. The default port is 22.

Example

```
rfs7000-37FABE(config-management-policy-test)#ssh port 162

rfs7000-37FABE(config-management-policy-test)#show context
management-policy test
 no http server
 https server
 ftp username superuser password 1
626b4033263d6d2ae4e79c48cdfcccb60fd4c77a8da9e365060597a6d6570ec2 rootdir dir
 ssh port 162
 snmp-server community snmp1 ro
 snmp-server user snmpmanager v3 encrypted des auth md5 0 motorola1123
 snmp-server host 172.16.10.23 v3 162
 aaa-login radius external
 aaa-login radius policy test
 idle-session-timeout 0
 restrict-access host 172.16.10.2 log all
rfs7000-37FABE(config-management-policy-test)#
```

Related Commands:

no	Resets SSH access port to factory default (port 22)

telnet

management-policy

Enables Telnet. Telnet provides a command line interface to a remote host over TCP. Telnet provides no encryption, but it does provide a measure of authentication. Telnet access is disabled by default.

By default Telnet, when enabled, uses *Transmission Control Protocol* (TCP) port 23. Use this command to change the TCP port.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
telnet {port <1-65535>}
```

Parameters

```
telnet {port <1-65535>}
```

telnet	Enables Telnet
port <1-65535>	Optional. Configures the Telnet port. This is the port used for Telnet connections. • <1-65535> – Sets a value from 1 - 165535. The default port is 23.

Example

```
rfs7000-37FABE(config-management-policy-test)#telnet port 200

rfs7000-37FABE(config-management-policy-test)#show context
management-policy test
 telnet port 200
 no http server
 https server
 ftp username superuser password 1
626b4033263d6d2ae4e79c48cdfcccb60fd4c77a8da9e365060597a6d6570ec2 rootdir dir
 ssh port 162
 snmp-server community snmp1 ro
 snmp-server user snmpmanager v3 encrypted des auth md5 0 motorola1123
 snmp-server host 172.16.10.23 v3 162
 aaa-login radius external
 aaa-login radius policy test
 idle-session-timeout 0
 restrict-access host 172.16.10.2 log all
rfs7000-37FABE(config-management-policy-test)#
```

Related Commands:

no	Disables Telnet

user

management-policy

Adds new user account

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
user <USERNAME> password [0 <PASSWORD>|1 <SHA1-PASSWORD>|<PASSWORD>]
          role
[helpdesk|monitor|network-admin|security-admin|superuser|system-admin|
          web-user-admin] access [all|console|ssh|telnet|web]
```

Parameters

```
user <USERNAME> password [0 <PASSWORD>|1 <SHA1-PASSWORD>|<PASSWORD>] role
[helpdesk|monitor|network-admin|security-admin|superuser|system-admin|web-use
r-admin] access [all|console|ssh|telnet|web]
```

user <USERNAME>	Adds new user account to this management policy • <USERNAME> – Sets the username
password [0 <PASSWORD>| 1 <SHA1-PASSWORD>| <PASSWORD>]	Configures a password • 0 <PASSWORD> – Sets a clear text password • 1 <SHA1-PASSWORD> – Sets the SHA1 hash of the password • <PASSWORD> – Sets the password
role	Configures the user role. The options are: • helpdesk – Helpdesk administrator. Performs troubleshooting tasks, such as clear statistics, reboot, create and copy technical support dumps. The helpdesk administrator can also create a guest user account and password for registration. These details can be e-mailed or sent as SMS to mobile phone. • monitor – Monitor. Has read-only access to the system. Can view configuration and statistics except for secret information • network-admin – Network administrator. Manages layer 2, layer 3, Wireless, RADIUS server, DHCP server, and Smart RF • security-admin – Security administrator. Modifies WLAN keys and passphrases • superuser – Superuser. Has full access, including halt and delete startup-config • system-admin – System administrator. Upgrades image, boot partition, time, and manages admin access • web-user-admin – Web user administrator. This role is used to create guest users and credentials. The Web user admin can access only the custom GUI screen and does not have access to the normal CLI and GUI.
access [all|console|ssh| telnet|web]	Configures the access type • all – Allows all types of access: console, SSH, Telnet, and Web • console – Allows console access only • ssh – Allows SSH access only • telnet – Allows Telnet access only • web – Allows Web access only

Example

```
rfs7000-37FABE(config-management-policy-test)#user TESTER password moto123
role
superuser access all

rfs7000-37FABE(config-management-policy-test)#show context
management-policy test
 telnet port 200
 no http server
 https server
 ftp username superuser password 1
626b4033263d6d2ae4e79c48cdfcccb60fd4c77a8da9e365060597a6d6570ec2 rootdir dir
 ssh port 162
 user TESTER password 1
737670e898600bcc42ee91aab93b568efa73ffee5f4d1e1b12262887ac3646bc role
superuser access all
 snmp-server community snmp1 ro
 snmp-server user snmpmanager v3 encrypted des auth md5 0 motorola1123
 snmp-server host 172.16.10.23 v3 162
 aaa-login radius external
 aaa-login radius policy test
 idle-session-timeout 0
 restrict-access host 172.16.10.2 log all
```

```
rfs7000-37FABE(config-management-policy-test)#
```

Related Commands:

no	Removes a user account

service

management-policy

Invokes service commands

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
service [prompt|show]
service [prompt crash-info|show cli]
```

Parameters

```
service [prompt crash-info|show cli]
```

service prompt crash-info	Updates CLI prompt settings • crash-info – Includes an asterix at the end of the prompt if the device has crash files in the flash:/crashinfo folder
service show cli	Displays running system information • cli – Displays the current mode's CLI tree

Example

```
rfs7000-37FABE(config-management-policy-test)#service show cli
Management Mode mode:
+-help [help]
  +-search
    +-WORD [help search WORD (|detailed|only-show|skip-show|skip-no)]
      +-detailed [help search WORD (|detailed|only-show|skip-show|skip-no)]
      +-only-show [help search WORD (|detailed|only-show|skip-show|skip-no)]
      +-skip-show [help search WORD (|detailed|only-show|skip-show|skip-no)]
      +-skip-no [help search WORD (|detailed|only-show|skip-show|skip-no)]
+-show
  +-commands [show commands]
  +-simulate
    +-stats [show simulate stats]
  +-eval
    +-WORD [show eval WORD]
  +-debugging [show debugging (|(on DEVICE-OR-DOMAIN-NAME))]
    +-cfgd [show debugging cfgd]
    +-on
      +-DEVICE-OR-DOMAIN-NAME [show debugging (|(on DEVICE-OR-DOMAIN-NAME))]
```

```
    +-fib [show debugging fib(|(on DEVICE-NAME))]
      +-on
        +-DEVICE-NAME [show debugging fib(|(on DEVICE-NAME))]
    +-wireless [show debugging wireless (|(on DEVICE-OR-DOMAIN-NAME))]
      +-on
--More--
```

Related Commands:

no	Disables the inclusion of an asterix indicator notifying the presence of crash files

Chapter

RADIUS-POLICY 17

This chapter summarizes the RADIUS group, server, and user policy commands in the CLI command structure.

Remote Authentication Dial-In User Service (RADIUS) is a client/server protocol and software that enables remote access servers to authenticate users and authorize their access to the network. RADIUS is a distributed client/server system that secures networks against unauthorized access. RADIUS clients send authentication requests to the local RADIUS server containing user authentication and network service access information.

RADIUS enables centralized management of authentication data (usernames and passwords). When a client attempts to associate to a network, the authentication request is sent to the local RADIUS server. The authentication and encryption of communications takes place through the use of a shared secret password (not transmitted over the network).

The local RADIUS server stores the user database locally, and can optionally use a remote user database. It ensures higher accounting performance. It allows the configuration of multiple users, and assigns policies for group authorization.

Controllers and access points allow enforcement of user-based policies. User policies include dynamic VLAN assignment and access based on time of day. A certificate is required for EAP TTLS,PEAP and TLS RADIUS authentication (configured with the RADIUS service).

Dynamic VLAN assignment is achieved based on the RADIUS server response. A user who associates to WLAN1 (mapped to VLAN1) can be assigned a different VLAN after RADIUS server authentication. This dynamic VLAN assignment overrides the WLAN's VLAN ID to which the user associates.

The chapter is organized into the following sections:

radius-group

RADIUS-POLICY

This section describes RADIUS user group configuration commands.

The local RADIUS server allows the configuration of user groups with common user policies. User group names and associated users are stored in the local database. The user ID in the received access request is mapped to the associated wireless group for authentication. The configuration of groups allows enforcement of the following policies that control user access:

- Assign a VLAN to the user upon successful authentication
- Define start and end of time (HH:MM) when the user is allowed to authenticate
- Define the SSID list to which a user, belonging to this group, is allowed to associate

- Define the days of the week the user is allowed to login
- Rate limit traffic (for non-management users)

RADIUS users are categorized into three groups: normal user, management user, and guest user. A RADIUS group not configured as management or guest is a normal user group. User access and role settings depends on the RADIUS group the user belongs.

Use the (config) instance to configure RADIUS group commands. This command creates a group within the existing RADIUS group. To navigate to the RADIUS group instance, use the following commands:

```
<DEVICE>(config)#radius-group <GROUP-NAME>

rfs7000-37FABE(config)#radius-group test
rfs7000-37FABE(config-radius-group-test)#?
Radius user group configuration commands:
  guest       Make this group a Guest group
  no          Negate a command or set its defaults
  policy      Radius group access policy configuration
  rate-limit  Set rate limit for group

  clrscr      Clears the display screen
  commit      Commit all changes made in this session
  do          Run commands from Exec mode
  end         End current mode and change to EXEC mode
  exit        End current mode and down to previous mode
  help        Description of the interactive help system
  revert      Revert changes
  service     Service Commands
  show        Show running system information
  write       Write running configuration to memory or terminal

rfs7000-37FABE(config-radius-group-test)#
```

NOTE
The RADIUS group name cannot exceed 32 characters, and cannot be modified as part of the group edit process.

Table 15 summarizes RADIUS group configuration commands.

TABLE 15 RADIUS-Group-Config Commands

Command	Description	Reference
guest	Enables guest access for the newly created group	page 1041
no	Negates a command or reverts settings to their default	page 1046
policy	Configures RADIUS group access policy parameters	page 1041
rate-limit	Sets the default rate limit per user in Kbps, and applies it to all enabled WLANs	page 1045
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394

TABLE 15 RADIUS-Group-Config Commands

Command	Description	Reference
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

guest

radius-group

Configures this group as a guest (non-management) group. A guest user group has temporary permissions to the controller's local RADIUS server. You can configure multiple guest user groups, each having a unique set of settings. Guest user groups cannot be made management groups with access and role permissions.

Guest users and policies are used for captive portal authorization to the network.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
guest
```

Parameters

None

Example

```
rfs7000-37FABE(config-radius-group-test)#guest

rfs7000-37FABE(config-radius-group-test)#show context
radius-group test
 guest
rfs7000-37FABE(config-radius-group-test)#
```

Related Commands:

no	Makes this group a non-guest group

policy

radius-group

Sets a RADIUS group's authorization settings, such as access day/time, WLANs etc.

NOTE
A user-based VLAN is effective only if dynamic VLAN authorization is enabled for the WLAN.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
policy [access|day|role|ssid|time|vlan]

policy vlan <1-4094>

policy access [all|console|ssh|telnet|web]
policy access [all|console|ssh|telnet|web] {(all|console|ssh|telnet|web)}

policy day [all|fr|mo|sa|su|th|tu|we|weekdays]
{(fr|mo|sa|su|th|tu|we|weekdays)}

policy role
[helpdesk|monitor|network-admin|security-admin|superuser|system-admin|
          web-user-admin]

policy ssid <SSID>

policy time start <HH:MM> end <HH:MM>
```

NOTE
Access and role settings are applicable only to a management group. They cannot be configured for a RADIUS non-management group.

Parameters

```
policy vlan <1-4094>
```

vlan <1-4094>	Sets the guest RADIUS group's VLAN ID from 1 - 4094. The VLAN ID is representative of the shared SSID each group member (user) employs to interoperate within the network (once authenticated by the local RADIUS server). This option applicable to a guest user group, which has guest access and temporary permissions to the local RADIUS server. The terms of the guest access can be set uniquely for each group. Guest user groups cannot be made management groups with unique access and role permissions. Enable dynamic VLAN assignment for the WLAN for the VLAN assignment to take effect.

	`policy access [all|console|ssh|telnet|web] {(all|console|ssh|telnet|web)}`
access	Configures access type for a management group. Management groups can be assigned unique access and role permissions. • all – Allows all access. Wireless client access to the console, ssh, telnet, and/or Web • console – Allows console access only • ssh – Allows SSH access only • telnet – Allows Telnet access only • web – Allows Web access only These parameters are recursive, and you can provide access to more than one component.
	`policy role [helpdesk|monitor|network-admin|security-admin|superuser|system-admin|web-user-admin]`
role [helpdesk|monitor|network-admin|security-admin|superuser|system-admin|web-user-admin]	Configures the role assigned to a management RADIUS group. If a group is listed as a management group, it may also have a unique role assigned. Available roles include: • helpdesk – Helpdesk administrator. Performs troubleshooting tasks, such as clear statistics, reboot, create and copy tech support dumps. The helpdesk administrator can also create a guest user account and password for registration. These details can be e-mailed or sent as SMS to a mobile phone. • monitor – Monitor. Has read-only access to the network. Can view configuration and statistics except for secret information • network-admin – Network administrator. has wired and wireless access to the network. Manages layer 2, layer 3, Wireless, RADIUS server, DHCP server, and Smart RF • security-admin – Security administrator. Has full read/write access to the network. Modifies WLAN keys and passphrases • superuser – Superuser. Has full access, including halt and delete startup config • system-admin – System administrator. Upgrades image, boot partition, time, and manages admin access • web-user-admin – Web user administrator. This role is used to create guest users and credentials. The web-user-admin can access only the custom GUI screen and does not have access to the normal CLI and GUI.
	`policy ssid <SSID>`
ssid <SSID>	Sets the *Service Set Identifier* (SSID) for this guest RADIUS group. Use this command to assign SSIDs that users within this RADIUS group are allowed to associate. Assign SSIDs of those WLANs only that the guest users need to access. This option is not available for a management group. • <SSID> – Sets a case-sensitive alphanumeric SSID, not exceeding 32 characters
	`policy day [all|fr|mo|sa|su|th|tu|we|weekdays] {(fr|mo|sa|su|th|tu|we|weekdays)}`
day [all|fr|mo|sa|su|th|tu|we|weekdays]	Configures the days on which this guest RADIUS group members can access the local RADIUS resources. The options are recursive, and you can provide access on multiple days. • fr – Allows access on Friday only • mo – Allows access on Mondays only • sa – Allows access on Saturdays only • su – Allows access on Sundays only • th – Allows access on Thursdays only • tu – Allows access on Tuesdays only • we – Allows access on Wednesdays only • weekdays – Allows access on weekdays only (Monday to Friday

	`policy time start <HH:MM> end <HH:MM>`
time start<HH:MM> end <HH:MM>	Configures the time when this RADIUS group can access the network • start <HH:MM> – Sets the start time in the HH:MM format (for example, 13:30 means the user can login only after 1:30 PM). Specifies the time users, within each listed group, can access the local RADIUS resources • end <HH:MM> – Sets the end time in the HH:MM format (for example, 17:30 means the user is allowed to remain logged in until 5:30 PM). Specifies the time users, within each listed group, lose access to the local RADIUS resources

Usage Guidelines:

A management group access policy provides:

- access details
- user roles
- policy's start and end time

The SSID, day, and VLAN settings are not applicable to a management user group.

Example

```
The following example shows a RADIUS guest group settings:

rfs7000-37FABE(config-radius-group-test)#policy time start 13:30 end 17:30
rfs7000-37FABE(config-radius-group-test)#policy day all
rfs7000-37FABE(config-radius-group-test)#policy vlan 1
rfs7000-37FABE(config-radius-group-test)#policy ssid motorolasol

rfs7000-37FABE(config-radius-group-test)#show context
radius-group test
 guest
 policy vlan 1
 policy ssid motorolasol
 policy day mo
 policy day tu
 policy day we
 policy day th
 policy day fr
 policy day sa
 policy day su
 policy time start 13:30 end 17:30
rfs7000-37FABE(config-radius-group-test)#

The following example shows a RADIUS management group settings:

rfs7000-37FABE(config-radius-group-management)#policy access console ssh
telnet
rfs7000-37FABE(config-radius-group-management)#policy role network-admin
rfs7000-37FABE(config-radius-group-management)#policy time start 9:30 end
20:30

rfs7000-37FABE(config-radius-group-management)#show context
radius-group management
 policy time start 9:30 end 20:30
 policy access console ssh telnet web
 policy role network-admin
rfs7000-37FABE(config-radius-group-management)#
```

Related Commands:

no	Removes or modifies a RADIUS group's access settings

rate-limit

radius-group

Sets the rate limit for the guest RADIUS server group

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
rate-limit [from-air|to-air] <100-1000000>
```

NOTE
The rate-limit setting is not applicable to a management group.

Parameters

```
rate-limit [from-air|to-air] <100-1000000>
```

to-air <100-1000000>	Sets the rate limit in the downlink direction, from the network to the wireless client • <100-1000000> – Sets the rate from 100 - 1000000 Kbps
from-air <100-1000000>	Sets the rate limit in the uplink direction, from the wireless client to the network • <100-1000000> – Sets the rate from 100 - 1000000 Kbps

Example

```
rfs7000-37FABE(config-radius-group-test)##rate-limit to-air 101

rfs7000-37FABE(config-radius-group-test)#show context
radius-group test
 guest
 policy vlan 1
 policy ssid motorolasol
 policy day mo
 policy day tu
 policy day we
 policy day th
 policy day fr
 policy day sa
 policy day su
 rate-limit to-air 200
 policy time start 13:30 end 17:30
rfs7000-37FABE(config-radius-group-test)#
```

Related Commands:

no	Removes the RADIUS guest group's rate limits

no

radius-group

Negates a command or sets its default. Removes or modifies the RADIUS group policy settings. When used in the config RADIUS group mode, the no command removes or modifies the following settings: access type, access days, role type, VLAN ID, and SSID.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no [guest|policy|rate-limit]

no policy [access|day|role|ssid|time|vlan]

no policy access [all|console|ssh|telnet|web]
no policy day [all|fr|mo|sa|su|th|tu|we|weekdays]
no policy ssid [<SSID>|all]
no policy [role|time|vlan]

no rate-limit [from-air|to-air]
```

Parameters

```
no guest
```

no guest	Makes a RADIUS guest group a non-guest (management) group

```
no policy access [all|console|ssh|telnet|web]
```

no policy access	Removes or modifies the RADIUS management group access • all – Removes all access (Wireless client access to the console, SSH, Telnet, and Web) • console – Removes console access • ssh – Removes SSH access • telnet – Removes Telnet • web – Removes Web access These are recursive options, and you can remove more than one at a time.

	`no policy day [all|fr|mo|sa|su|th|tu|we|weekdays]`
no policy days	Removes or modifies the days on which access is provided to a RADIUS guest group • all – Removes access on all days (Monday to Sunday) • fr – Removes access on Fridays only • mo – Removes access on Mondays only • sa – Removes access on Saturdays only • su – Removes access on Sundays only • th – Removes access on Thursdays only • tu – Removes access on Tuesdays only Contd..
	• we – Removes access on Wednesdays only • weekdays – Removes access on weekdays (Monday to Friday) These are recursive options, and you can remove more than one at a time.
	`no policy ssid [<SSID>|all]`
no policy ssid	Removes a SSID assigned to a RADIUS guest group • <SSID> – Specify the RADIUS group SSID. RADIUS group users will not be allowed access to the WLAN represented by the specified SSID. • all – Removes all allowed WLANs
	`no policy [role|time|vlan]`
no policy role	Removes the RADIUS management group's role
no policy time	Removes the RADIUS guest group's start and end access time
no policy vlan	Removes the RADIUS guest group's VLAN ID
	`no rate-limit [from-air|to-air]`
no rate-limit	Removes RADIUS guest group's rate limit
from-air	Removes the uplink (from wireless client to network) rate limit
to-air	Removes the downlink (from network to wireless client) rate limit

Example

```
The following example shows the RADIUS guest group 'test' settings before the
'no' commands are executed:

rfs7000-37FABE(config-radius-group-test)#show context
radius-group test
 guest
 policy vlan 1
 policy ssid motorolasol
 policy day mo
 policy day tu
 policy day we
 policy day th
 policy day fr
 policy day sa
 policy day su
 rate-limit to-air 200
 policy time start 13:30 end 17:30
rfs7000-37FABE(config-radius-group-test)#

rfs7000-37FABE(config-radius-group-test)#no guest
rfs7000-37FABE(config-radius-group-test)#no rate-limit to-air
```

```
rfs7000-37FABE(config-radius-group-test)#no policy day all

The following example shows the RADIUS guest group ‘test’ settings after the
‘no’ commands are executed:

rfs7000-37FABE(config-radius-group-test)#show context
radius-group test
 policy vlan 1
 policy ssid motorolasol
 policy time start 13:30 end 17:30
rfs7000-37FABE(config-radius-group-test)#
```

Related Commands:

guest	Manages a guest user linked with a captive portal
policy	Sets a RADIUS group’s authorization policies
rate-limit	Sets a RADIUS group’s rate limit

radius-server-policy

RADIUS-POLICY

Creates an onboard device RADIUS server policy.

A RADIUS server policy is a unique authentication and authorization configuration that receives user connection requests, authenticates users, and returns configuration information necessary for the RADIUS client to deliver service to the user. The client is the entity with authentication information requiring validation. The local RADIUS server has access to a database of authentication information used to validate the client's authentication request.

The local RADIUS server uses authentication schemes like PAP, CHAP, or EAP to verify and confirm information provided by a user. The user's proof of identification is verified, along with, optionally, other information. A local RADIUS server policy can also be configured to refer to an external *Lightweight Directory Access Protocol* (LDAP) resource to verify a user's credentials.

Use the (config) instance to configure RADIUS-Server-Policy related parameters. To navigate to the RADIUS-Server-Policy instance, use the following commands:

```
<DEVICE>(config)#radius-server-policy <POLICY-NAME>

rfs7000-37FABE(config)#radius-server-policy test
rfs7000-37FABE(config-radius-server-policy-test)#?
Radius Configuration commands:
  authentication           Radius authentication
  chase-referral           Enable chasing referrals from LDAP server
  crl-check                Enable Certificate Revocation List( CRL ) check
  ldap-agent               LDAP Agent configuration parameters
  ldap-group-verification  Enable LDAP Group Verification setting
  ldap-server              LDAP server parameters
  local                    RADIUS local realm
  nas                      RADIUS client
  no                       Negate a command or set its defaults
  proxy                    RADIUS proxy server
  session-resumption       Enable session resumption/fast reauthentication by
                           using cached attributes
  use                      Set setting to use
```

```
  clrscr                  Clears the display screen
  commit                  Commit all changes made in this session
  do                      Run commands from Exec mode
  end                     End current mode and change to EXEC mode
  exit                    End current mode and down to previous mode
  help                    Description of the interactive help system
  revert                  Revert changes
  service                 Service Commands
  show                    Show running system information
  write                   Write running configuration to memory or terminal

rfs7000-37FABE(config-radius-server-policy-test)#
```

The following table summarizes RADIUS server policy configuration commands.

Commands	Description	Reference
authentication	Configures RADIUS authentication settings	page 1049
chase-referral	Enables LDAP server referral chasing	page 1051
crl-check	Enables a *certificate revocation list* (CRL) check	page 1052
ldap-agent	Configures the LDAP agent's settings	page 1052
ldap-group-verification	Enables LDAP group verification	page 1055
ldap-server	Configures the LDAP server's settings	page 1055
local	Configures a local RADIUS realm	page 1057
nas	Configures the key sent to a RADIUS client	page 1058
no	Removes or resets the RADIUS server policy's settings	page 1059
proxy	Configures the RADIUS proxy server's settings	page 1062
session-resumption	Enables session resumption	page 1064
use	Defines settings used with the RADIUS server policy	page 1065
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

authentication

radius-server-policy

Specifies the RADIUS datasource used for user authentication. Options include local for the local user database or LDAP for a remote LDAP resource.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
authentication [data-source|eap-auth-type]

authentication data-source [ldap|local]
authentication data-source [ldap {fallack}|local] {(ssid <SSID> precedence
<1-5000>)}

authentication eap-auth-type
[all|peap-gtc|peap-mschapv2|tls|ttls-md5|ttls-mschapv2|
          ttls-pap]
```

Parameters

```
authentication data-source [ldap {fallback}|local] {(ssid <SSID> precedence
<1-5000>)}
```

data-source	The RADIUS sever can either use the local database or an external LDAP server to authenticate a user. It is necessary to specify the data source. The options are: LDAP and local. **NOTE:** The default setting is local.
ldap fallback	Uses a remote LDAP server as the data source • fallback – Optional. Enables fallback to local authentication. This feature ensures that when the configured LDAP data source is unreachable, the client is authenticated against the local RADIUS resource. This option is disabled by default.
local	Uses the local user database to authenticate a user
ssid <SSID> precedence <1-5000>	The following keywords are recursive and common to both 'ldap' and 'local' parameters: • ssid – Optional. Associates the data source, selected in the previous step, with a SSID. • <SSID> – Specify the SSID for this authentication data source. The SSID is case sensitive and should not exceed 32 characters in length. Do not use any of the following characters (**< > | " & \ ? ,**). • precedence <SSID> – Sets the precedence for this authentication rule. The precedence value allows systematic evaluation and application of rules. Rules with the lowest precedence receive the highest priority. • <1-5000> – Specify a precedence from 1 -5000. Specifying the SSID allows the RADIUS server to use the SSID attribute in access requests to determine the data source to use. This option is applicable to onboard RADIUS servers only.

```
authentication eap-auth-type [all|peap-gtc|peap-mschapv2|tls|ttls-md5|
ttls-mschapv2|ttls-pap]
```

eap-auth-type	Uses *Extensible Authentication Protocol* (EAP), with this RADIUS server policy, for user authentication The EAP authentication types supported by the local RADIUS server are: all, peap-gtc, peap-mschapv2, tls, ttls-md5, ttls-mschapv2, ttls-pap.
all	Enables both TTLS and PEAP authentication

peap-gtc	Enables PEAP with default authentication using GTC
peap-mschapv2	Enables PEAP with default authentication using MSCHAPv2
tls	Enables TLS as the EAP type
ttls-md5	Enables TTLS with default authentication using md5
ttls-mschapv2	Enables TTLS with default authentication using MSCHAPv2
ttls-pap	Enables TTLS with default authentication using PAP

Example

```
rfs7000-37FABE(config-radius-server-policy-test)#authentication eap-auth-type
tls

rfs7000-37FABE(config-radius-server-policy-test)#show context
radius-server-policy test
 authentication eap-auth-type tls
rfs7000-37FABE(config-radius-server-policy-test)#
```

Related Commands:

no	Removes the RADIUS authentication settings

chase-referral

radius-server-policy

Enables chasing of referrals from an external LDAP server resource

An LDAP referral is a controller or service platform's way of indicating to a client it does not hold the section of the directory tree where a requested content object resides. The referral is the controller or service platform's direction to the client a different location is more likely to hold the object, which the client uses as the basis for a DNS search for a domain controller. Ideally, referrals always reference a domain controller that indeed holds the object. However, it is possible for the domain controller to generate another referral, although it usually does not take long to discover the object does not exist and inform the client.

This feature is disabled by default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
chase-referral
```

Parameters

None

Example

```
rfs7000-37FABE(config-radius-server-policy-test)#chase-referral
```

Related Commands:

no	Disables LDAP server referral chasing

crl-check

radius-server-policy

Enables a *certificate revocation list* (CRL) check on this RADIUS server policy

A CRL is a list of revoked certificates issued and subsequently revoked by a *Certification Authority* (CA). Certificates can be revoked for a number of reasons including failure or compromise of a device using a certificate, a compromise of a certificate key pair or errors within an issued certificate. The mechanism used for certificate revocation depends on the CA.

This option is disabled by default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
crl-check
```

Parameters

None

Example

```
rfs7000-37FABE(config-radius-server-policy-test)#crl-check

rfs7000-37FABE(config-radius-server-policy-test)#show context
radius-server-policy test
 authentication eap-auth-type tls
 crl-check
rfs7000-37FABE(config-radius-server-policy-test)#
```

Related Commands:

no	Disables CRL check on a RADIUS server policy

ldap-agent

radius-server-policy

Configures the LDAP agent's settings in the RADIUS server policy context

When a user's credentials are stored on an external LDAP server, the local RADIUS server cannot successfully conduct PEAP-MSCHAPv2 authentication, since it is not aware of the user's credentials maintained on the external LDAP server resource. Therefore, up to two LDAP agents can be provided locally so remote LDAP authentication can be successfully accomplished on the remote LDAP resource (using credentials maintained locally).

This feature is available to all controller, service platforms and access point models, with the exception of Brocade Mobility 6511 Access Point running in standalone AP or virtual controller AP mode. However, this feature is supported by dependent mode Brocade Mobility 6511 Access Point access points when adopted and managed by a controller or service platform.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
ldap-agent [join|join-retry-timeout|primary|secondary]

ldap-agent [join {on <DEVICE-NAME>}|join-retry-timeout <60-300>]

ldap-agent [primary|secondary] domain-name <LDAP-DOMAIN-NAME>
domain-admin-user
          <ADMIN-USER-NAME> domain-admin-password [0 <WORD>|2 <WORD>]
```

Parameters

```
ldap-agent [join {on <DEVICE-NAME>}|join-retry-timeout <60-300>]
```

ldap-agent	Configures the LDAP agent's settings
join {on <DEVICE-NAME>}	Initiates the join process, which binds the RADIUS server with the LDAP server's (Windows) domain. When successful, the hostname (name of the AP, wireless controller, or service platform) is added to the LDAP server's Active Directory. • on <DEVICE-NAME> – Optional. Specifies the device name • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. To confirm the join status of a controller, use the *show* > *ldap-agent* > *join-status* command.
join-retry-timeout <60-300>	If the join process fails (i.e. the RADIUS server fails to join the LADP server's domain), the process is retried after a specified interval. This command configures the interval (in seconds) between two successive join attempts. • <60-300> – Set the timeout value from 60 - 300 seconds. The default is 60 seconds. A retry timer is initiated as soon as the join process starts, which tracks the time lapse in case of a failure.

```
ldap-agent [primary|secondary] domain-name <LDAP-DOMAIN-NAME>
domain-admin-user
<ADMIN-USER-NAME> domain-admin-password [0 <WORD>|2 <WORD>]
```

ldap-agent	Configures the LDAP agent's settings
primary	Configures the primary LDAP server details, such as domain name, user name, and password. The RADIUS server uses these credentials to bind with the primary LDAP server.
secondary	Configures the secondary LDAP server details, such as domain name, user name, and password. The RADIUS server uses these credentials to bind with the secondary LDAP server.

domain-name <LDAP-DOMAIN-NAME>	This keyword is common to both the 'primary' and 'secondary' parameters. • domain-name – Configures the primary or secondary LDAP server's domain name • <LDAP-DOMAIN-NAME> – Specify the domain name.
domain-admin-user <ADMIN-USER-NAME>	This keyword is common to both the 'primary' and 'secondary' parameters. • domain-admin-user – Configures the primary or secondary LDAP server's admin user name • <ADMIN-USER-NAME> – Specify the admin user's name.

domain-admin-password [0 <WORD>|2 <WORD>]	This keyword is common to both the 'primary' and 'secondary' parameters.
	• domain-admin-password – Configures the primary or secondary LDAP server's admin user password
	  • 0 <WORD> – Specifies the password in the unencrypted format
	  • 2 <WORD> – Specifies the password in the encrypted format

Example

```
rfs4000-229D58(config-radius-server-policy-test)#ldap-agent primary
domain-name
symbol domain-admin-user Administrator domain-admin-password 0 Symbol@123
rfs4000-229D58(config-radius-server-policy-test)#

rfs4000-229D58(config-radius-server-policy-test)#show context
radius-server-policy test
 ldap-agent primary domain-name symbol domain-admin-user Administrator
domain-admin-password 0 Symbol@123
rfs4000-229D58(config-radius-server-policy-test)#

rfs4000-229D58(config)#show session-config
!
! Configuration of Brocade Mobility RFS4000 version 5.5.0.0-038B
!
!
version 2.3
!
.............................................................
meshpoint test
 meshid test
 beacon-format mesh-point
 control-vlan 1
 security-mode none
 no root
!
smart-rf-policy test
!
wips-policy test
!
radius-server-policy test
 ldap-agent primary domain-name symbol domain-admin-user Administrator
domain-admin-password 0 Symbol@123
!
!
--More--
rfs4000-229D58(config)#
```

Related Commands:

no	Removes LDAP agent settings from this RADIUS server policy

ldap-group-verification

radius-server-policy

Enables LDAP group verification settings on this RADIUS server policy

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
ldap-group-verification
```

Parameters

None

Example

```
rfs7000-37FABE(config-radius-server-policy-test)#ldap-group-verification
rfs7000-37FABE(config-radius-server-policy-test)#
```

Related Commands:

no	Disables LDAP group verification settings

ldap-server

radius-server-policy

Configures the LDAP server's settings. Configuring LDAP server allows users to login and authenticate from anywhere on the network.

Administrators have the option of using the local RADIUS server to authenticate users against an external LDAP server resource. Using an external LDAP user database allows the centralization of user information and reduces administrative user management overhead making RADIUS authorization more secure and efficient.

RADIUS is not just a database. It is a protocol for asking intelligent questions to a user database (like LDAP). LDAP however is just a database of user credentials used optionally with the local RADIUS server to free up resources and manage user credentials from a secure remote location. It is the local RADIUS resources that provide the tools to perform user authentication and authorize users based on complex checks and logic. A LDAP user database alone cannot perform such complex authorization checks.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
ldap-server [dead-period|primary|secondary]

ldap-server dead-period <0-600>

ldap-server [primary|secondary] host <IP> port <1-65535> login <LOGIN-NAME>
          bind-dn <BIND-DN> base-dn <BASE-DN> passwd [0 <PASSWORD>|2
<ENCRYPTED-PASSWORD>|
          <PASSWORD>] passwd-attr <ATTR> group-attr <ATTR> group-filter
<FILTER>
          group-membership <WORD> {net-timeout <1-10>}
```

Parameters

```
ldap-server dead-period <0-600>
```

dead-period <0-600>	Set an interval, in seconds, during which the local server will not contact its LDAP server resource once its been defined as unavailable. A dead period is only implemented when additional LDAP servers are configured and available. • <0-600> – Specify a value from 0 - 600 seconds.

```
ldap-server [primary|secondary] host <IP> port <1-65535> login <LOGIN-NAME>
bind-dn <BIND-DN> base-dn <BASE-DN> passwd [0 <PASSWORD>|2
<ENCRYPTED-PASSWORD>|
<PASSWORD>] passwd-attr <ATTR> group-attr <ATTR> group-filter <FILTER>
group-membership <WORD> {net-timeout <1-10>}
```

ldap primary	Configures the primary LDAP server settings
ldap secondary	Configures the secondary LDAP server settings
host <IP>	Specifies the LDAP host IP address • <IP> – Specify the LDAP server's IP address.
port <1-65535>	Configures the LDAP server port • <1-65535> – Specify a port between 1 - 65535.
login <LOGIN-NAME>	Configures the login name of a user to access the LDAP server • <LOGIN-NAME> – Specify a login ID (should not exceed 127 characters).
bind-dn <BIND-DN>	Configures a distinguished bind name. This is the *distinguished name* (DN) used to bind with the LDAP server. The DN is the name that uniquely identifies an entry in the LDAP directory. A DN is made up of attribute value pairs, separated by commas. • <BIND-DN> – Specify a bind name (should not exceed 127 characters).
base-dn <BASE-DN>	Configures a distinguished base name. This is the DN that establishes the base object for the search. The base object is the point in the LDAP tree at which to start searching. LDAP DNs begin with a specific attribute (usually some sort of name), and continue with progressively broader attributes, often ending with a country attribute. The first component of the DN is referred to as the *Relative Distinguished Name* (RDN). It identifies an entry distinctly from any other entries that have the same parent • <BASE-DN> – Specify a base name (should not exceed 127 characters).
passwd [0 <PASSWORD>| 2 <ENCRYPTED-PASSWORD>| <PASSWORD>]	Sets a valid password for the LDAP server. • 0 <PASSWORD> – Sets an UNENCRYPTED password • 2 <PASSWORD> – Sets an ENCRYPTED password • <PASSWORD> – Sets the LDAP server bind password, specified UNENCRYPTED, with a maximum size of 31 characters

passwd-attr <ATTR>	Specify the LDAP server password attribute (should not exceed 63 characters).
group-attr <ATTR>	Specify a name to configure group attributes (should not exceed 31 characters). LDAP systems have the facility to poll dynamic groups. In an LDAP dynamic group an administrator can specify search criteria. All users matching the search criteria are considered a member of this dynamic group. Specify a group attribute used by the LDAP server. An attribute could be a group name, group ID, password or group membership name.
group-filter <FILTER>	Specify a name for the group filter attribute (should not exceed 255 characters). This filter is typically used for security role-to-group assignments and specifies the property to look up groups in the directory service.
group-membership <WORD>	Specify a name for the group membership attribute (should not exceed 63 characters). This attribute is sent to the LDAP server when authenticating users.
net-time <1-10>	Optional. Select a value from 1 - 10 to configure the network timeout (number of seconds to wait for a response from the target primary or secondary LDAP server). The default is 10 seconds.

Example

```
rfs7000-37FABE(config-radius-server-policy-test)#ldap-server dead-period 100

rfs7000-37FABE(config-radius-server-policy-test)#ldap-server primary host
172.16
.10.19 port 162 login motorolasol bind-dn bind-dn1 base-dn base-dn1 passwd 0
motorolasol@123 passwd-attr moto123 group-attr group1 group-filter
groupfilter1
group-membership groupmembership1 net-timeout 2
rfs7000-37FABE(config-radius-server-policy-test)#

rfs7000-37FABE(config-radius-server-policy-test)#show context
radius-server-policy test
 authentication eap-auth-type tls
 crl-check
 ldap-server primary host 172.16.10.19 port 162 login "motorolasol" bind-dn
"bind-dn1" base-dn "base-dn1" passwd 0 motorolasol@123 passwd-attr moto123
group-attr group1 group-filter "groupfilter1" group-membership
groupmembership1 net-timeout 2
 ldap-server dead-period 100
rfs7000-37FABE(config-radius-server-policy-test)#
```

Related Commands:

no	Disables the LDAP server parameters

local

radius-server-policy

Configures a local RADIUS realm on this RADIUS server policy

When the local RADIUS server receives a request for a user name with a realm, the server references a table of realms. If the realm is known, the server proxies the request to the RADIUS server.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
local realm <RADIUS-REALM>
```

Parameters

```
local realm <RADIUS-REALM>
```

realm <RADIUS-REALM>	Configures a local RADIUS realm • <RADIUS-REALM> – Sets a local RADIUS realm name (a string not exceeding 50 characters)

Example

```
rfs7000-37FABE(config-radius-server-policy-test)#local realm realm1

rfs7000-37FABE(config-radius-server-policy-test)#show context
radius-server-policy test
 authentication eap-auth-type tls
 crl-check
 local realm realm1
 ldap-server primary host 172.16.10.19 port 162 login "motorolasol" bind-dn
"bind-dn1" base-dn "base-dn1" passwd 0 motorolasol@123 passwd-attr moto123
group-attr group1 group-filter "groupfilter1" group-membership
groupmembership1 net-timeout 2
 ldap-server dead-period 100
rfs7000-37FABE(config-radius-server-policy-test)#
```

Related Commands:

no	Removes the RADIUS local realm

nas

radius-server-policy

Configures the key sent to a RADIUS client

A RADIUS client is a mechanism to communicate with a central server to authenticate users and authorize access to the controller, service platform or Access Point managed network.

The client and server share a secret (a password). That shared secret followed by the request authenticator is put through a MD5 hash algorithm to create a 16 octet value which is XORed with the password entered by the user. If the user password is greater than 16 octets, additional MD5 calculations are performed, using the previous ciphertext instead of the request authenticator. The server receives a RADIUS access request packet and verifies the server possesses a shared secret for the client. If the server does not possess a shared secret for the client, the request is dropped. If the client received a verified access accept packet, the username and password are considered correct, and the user is authenticated. If the client receives a verified access reject message, the username and password are considered to be incorrect, and the user is not authenticated.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
nas <IP/M> secret [0|2|<LINE>]

nas <IP/M> secret [0 <LINE>|2 <LINE>|<LINE>]
```

Parameters

```
nas <IP/M> secret [0 <LINE>|2|<LINE>]
```

<IP/M>	Sets the RADIUS client's IP address • <IP/M> – Sets the RADIUS client's IP address in the A.B.C.D/M format
secret [0 <LINE>|2 <LINE>| <LINE>]	Sets the RADIUS client's shared secret. Use one of the following options: • 0 <LINE> – Sets an UNENCRYPTED secret • 2 <LINE> – Sets an ENCRYPTED secret • <LINE> – Defines the secret (client shared secret) up to 64 characters

Example

```
rfs7000-37FABE(config-radius-server-policy-test)#nas 172.16.10.10/24 secret 0
wirelesswell

rfs7000-37FABE(config-radius-server-policy-test)#show context
radius-server-policy test
 authentication eap-auth-type tls
 crl-check
 nas 172.16.10.10/24 secret 0 wirelesswell
 local realm realm1
 ldap-server primary host 172.16.10.19 port 162 login "motorolasol" bind-dn
"bind-dn1" base-dn "base-dn1" passwd 0 motorolasol@123 passwd-attr moto123
group-attr group1 group-filter "groupfilter1" group-membership
groupmembership1 net-timeout 2
 ldap-server dead-period 100
rfs7000-37FABE(config-radius-server-policy-test)#
```

Related Commands:

no	Removes a RADIUS server's client on a RADIUS server policy

no

radius-server-policy

Negates a command or reverts back to default settings. When used with in the config RADIUS server policy mode, the no command removes settings, such as crl-check, LDAP group verification, RADIUS client etc.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no
[authentication|chase-referral|clr-check|ldap-agent|ldap-group-verification|
          ldap-server|local|nas|proxy|session-resumption|use]

no authentication [data-source|eap]
no authentication [data-source {ldap {fallback}|local|ssid}|eap configuration]

no [chase-referral|clr-check|ldap-group-verification|nas
<IP/M>|session-resumption]

no ldap-agent [join-retry-timeout|primary|secondary]

no local realm [<REALM-NAME>|all]

no proxy [realm <REALM-NAME>|retry-count|retry-delay]

no ldap-server [dead-period|primary|secondary]

no use [radius-group [<RAD-GROUP-NAME>|all]|radius-user-pool-policy
          [<RAD-USER-POOL-NAME>|all]]
```

Parameters

`no authentication [data-source {ldap {fallback}|local}|eap configuration]`

no authentication	Removes the RADIUS authentication settings
data-source {ldap fallback|local} {ssid <SSID> precedence <1-5000>}	Removes configured data source • ldap fallback – Optional. Removes a remote LDAP server as the data source for user authentication • fallback – Optional. Disables fallback to local authentication in case LDAP authentication fails • local – Optional. Removes a local database as the source of user authentication The following keywords are recursive and common to both 'ldap' and 'local' parameters: • ssid – Optional. Removes the SSID associated with this LDAP data source. • <SSID> – Specify the SSID. • precedence <SSID> – resets the precedence for this LDAP authentication rule. • <1-5000> – Specify the precedence from 1 -5000. Use this option to configure different data sources for each SSID.
eap configuration	Resets EAP authentication to the default mode

`no [chase-referral|clr-check|ldap-group-verification|nas <IP/M>|session-resumption]`

no chase-referral	Disables LDAP server referral chasing
no crl-check	Removes the CRL check
no ldap-group-verification	Disables a RADIUS server's LDAP group verification settings

no nas	Removes a RADIUS server's client • <IP/M> – Sets the IP address of the RADIUS client in the A.B.C.D/M format
no session-resumption	Disables a RADIUS server's session resumption settings

`no ldap-agent [join-retry-timeout|primary|secondary]`

no ldap-agent	Removes the LDAP agent parameters on this RADIUS server policy
join-retry-timeout	Removes the configured retry interval (this is the interval, in seconds, after which a access point or wireless controller retries joining the LDAP server's domain)
primary	Removes the primary LDAP server details (such as, domain name, admin user name, and password)
secondary	Removes the secondary LDAP server details (such as, domain name, admin user name, and password)

`no local realm [<REALM-NAME>|all]`

no local	Removes a RADIUS server's local realm
realm [<REALM-NAME>|all]	Removes a specified realm (specified by the <REALM-NAME> parameter) or all configured realms

`no proxy [realm <REALM-NAME>|retry-count|retry-delay]`

no proxy	Removes a RADIUS proxy server's settings
realm <REALM-NAME>	Removes a proxy server's realm name (specified by the <REALM-NAME> parameter)
retry-count	Removes a proxy server's retry count
retry-delay	Removes a proxy server's retry delay count

`no ldap-server [dead-period|primary|secondary]`

no ldap-server	Disables the LDAP server parameters
dead-period	Sets the dead period as the duration the RADIUS server will not contact the LDAP server after finding it unavailable.
primary	Removes the primary LDAP server
secondary	Removes the secondary LDAP server

`no use [radius-group [<RAD-GROUP-NAME>|all]|radius-user-pool-policy [<RAD-USER-POOL-NAME>|all]]`

no use	Removes the RADIUS group or a RADIUS user pool policy
radius-group <RAD-GROUP-NAME>	Removes a specified RADIUS group or all RADIUS groups • <RAD-GROUP-NAME> – Specify the RADIUS group name. • all – Removes all RADIUS groups
radius-user-pool-policy [<RAD-USER-POOL-NAME>|all]	Removes a specified RADIUS user pool or all RADIUS user pools • <RAD-USER-POOL-NAME> – Specify the RADIUS user pool name. • all – Removes all RADIUS user pools

Example

```
The following example shows the RADIUS server policy 'test' settings before
the 'no' commands are executed:

rfs7000-37FABE(config-radius-server-policy-test)#show context
radius-server-policy test
 authentication eap-auth-type tls
```

```
 crl-check
 nas 172.16.10.10/24 secret 0 wirelesswell
 local realm realm1
 ldap-server primary host 172.16.10.19 port 162 login "motorolasol" bind-dn
"bind-dn1" base-dn "bas-dn1" passwd 0 motorolasol@123 passwd-attr moto123
group-attr group1 group-filter "groupfilter1" group-membership
groupmembership1 net-timeout 2
 ldap-server dead-period 100
rfs7000-37FABE(config-radius-server-policy-test)#

rfs7000-37FABE(config-radius-server-policy-test)#no authentication eap
configuration
rfs7000-37FABE(config-radius-server-policy-test)#no crl-check
rfs7000-37FABE(config-radius-server-policy-test)#no local realm realm1
rfs7000-37FABE(config-radius-server-policy-test)#no nas 172.16.10.10/24
rfs7000-37FABE(config-radius-server-policy-test)#no ldap-server dead-period

The following example shows the RADIUS server policy ‘test’ settings after the
‘no’ commands are executed:

rfs7000-37FABE(config-radius-server-policy-test)#show context
radius-server-policy test
 ldap-server primary host 172.16.10.19 port 162 login "motorolasol" bind-dn
"bind-dn1" base-dn "bas-dn1" passwd 0 motorolasol@123 passwd-attr moto123
group-attr group1 group-filter "groupfilter1" group-membership
groupmembership1 net-timeout 2
rfs7000-37FABE(config-radius-server-policy-test)#
```

Related Commands:

authentication	Configures RADIUS server authentication parameters
chase-referral	Enables LDAP server referral chasing
crl-check	Enables a CRL check
ldap-agent	Configures the LDAP agent’s parameters
ldap-group-verification	Enables LDAP group verification settings
ldap-server	Configures the LDAP server parameters. Configuring the LDAP server allows users to login and authenticate from anywhere on the network
local	Configures a local RADIUS realm on this RADIUS server policy
nas	Configures the key sent to a RADIUS client
proxy	Configures a proxy RADIUS server based on the realm/suffix
session-resumption	Enables session resumption/fast re-authentication by using cached attributes
use	Defines settings used with the RADIUS server policy

proxy

radius-server-policy

Configures a proxy RADIUS server based on the realm/suffix. The realm identifies where the RADIUS server forwards AAA requests for processing.

A user's access request is sent to a proxy RADIUS server if it cannot be authenticated by the local RADIUS resources. The proxy server checks the information in the user access request and either accepts or rejects the request. If the proxy server accepts the request, it returns configuration information specifying the type of connection service required to authenticate the user.

The RADIUS proxy appears to act as a RADIUS server to NAS, whereas the proxy appears to act as a RADIUS client to the RADIUS server.

When the proxy server receives a request for a user name with a realm, the server references a table of realms. If the realm is known, the server proxies the request to the RADIUS server.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
proxy [realm|retry-count|retry-delay]

proxy realm <REALM-NAME> server <IP> port <1024-65535> secret
          [0 <PASSWORD>|2 <ENCRYPTED-PASSWORD>|<PASSWORD>]

proxy retry-count <3-6>

proxy retry-delay <5-10>
```

Parameters

```
proxy realm <REALM-NAME> server <IP> port <1024-65535> secret
[0 <PASSWORD>|2 <ENCRYPTED-PASSWORD>|<PASSWORD>]
```

proxy realm <REALM-NAME>	Configures the realm name • <REALM-NAME> – Specify the realm name. The name should not exceed 50 characters.
server <IP>	Configures the proxy server's IP address. This is the address of server checking the information in the user access request and either accepting or rejecting the request on behalf of the local RADIUS server. • <IP> – Sets the proxy server's IP address
port <1024-65535>	Configures the proxy server's port. This is the TCP/IP port number for the server that acts as a data source for the proxy server. • <1024-65535> – Sets the proxy server's port from 1024 - 65535 (default port is 1812)
secret [0 <PASSWORD>| 2 <ENCRYPTED-PASSWORD>| <PASSWORD>	Sets the proxy server secret string. The options are: • 0 <PASSWORD> – Sets an UNENCRYPTED password • 2 <ENCRYPTED-PASSWORD> – Sets an ENCRYPTED password • <PASSWORD> – Sets the proxy server shared secret value

```
proxy retry-count <3-6>
```

retry-count <3-6>	Sets the proxy server's retry count. This is the maximum number attempts made by a controllers RDIUS server to connect to the proxy server. • <3-6> – Sets a value from 3 - 6 (default is 3 counts)

```
proxy retry-delay <5-10>
```

retry-delay <5-10>	Sets the proxy server's retry delay count. This is the interval the controller's RADIUS server waits before making an additional connection attempt. • <5-10> – Sets a value from 5 - 10 seconds (default is 5 seconds)

Usage Guidelines:

A maximum of five RADIUS proxy servers can be configured. The proxy server attempts six retries before it times out. The retry count defines the number of times RADIUS requests are transmitted before giving up. The timeout value is the defines the interval between successive retransmission of a RADIUS request (in case of no reply).

Example

```
rfs7000-37FABE(config-radius-server-policy-test)#proxy realm test1 server
172.16
.10.7 port 1025 secret 0 motorolaSol1123

rfs7000-37FABE(config-radius-server-policy-test)#proxy retry-count 4

rfs7000-37FABE(config-radius-server-policy-test)#proxy retry-delay 8

rfs7000-37FABE(config-radius-server-policy-test)#show context
radius-server-policy test
 proxy retry-delay 8
 proxy retry-count 4
 proxy realm test1 server 172.16.10.7 port 1025 secret 0 motorolaSol1123
 ldap-server primary host 172.16.10.19 port 162 login "motorolasol" bind-dn
"bind-dn1" base-dn "bas-dn1" passwd 0 motorolasol@123 passwd-attr moto123
group-attr group1 group-filter "groupfilter1" group-membership
groupmembership1 net-timeout 2
rfs7000-37FABE(config-radius-server-policy-test)#
```

Related Commands:

no	Removes or resets the RADIUS proxy server's settings

session-resumption

radius-server-policy

Enables session resumption or fast re-authentication by using cached attributes. This feature controls the volume and duration cached data is maintained by the server policy, upon termination of a server policy session. The availability and quick retrieval of the cached data speeds up session resumption.

This feature is disabled by default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
session-resumption {lifetime|max-entries}

session-assumption {lifetime <1-24> {max-entries <10-1024>}|max-entries
<10-1024>}
```

Parameters

```
session-assumption {lifetime <1-24> {max-entries <10-1024>}|
max-entries <10-1024>}
```

lifetime <1-24> {max-entries <10-1024>}	Optional. Sets the lifetime of cached entries • <1-24> – Specify the lifetime period from 1 - 24 hours (default is 1 hour) • max-entries – Optional. Configures the maximum number of entries in the cache • <10-1024> – Sets the maximum number of entries in the cache from 10 - 1024 (default is 128 entries)
max-entries <10-1024>	Optional. Configures the maximum number of entries in the cache • <10-1024> – Sets the maximum number of entries in the cache from 10 - 1024 (default is 128 entries)

Example

```
rfs7000-37FABE(config-radius-server-policy-test)#session-resumption lifetime
10
max-entries 11

rfs7000-37FABE(config-radius-server-policy-test)#show context
radius-server-policy test
 proxy retry-delay 8
 proxy retry-count 4
 proxy realm test1 server 172.16.10.7 port 1025 secret 0 motorolaSol1123
 ldap-server primary host 172.16.10.19 port 162 login "motorolasol" bind-dn
"bind-dn1" base-dn "bas-dn1" passwd 0 motorolasol@123 passwd-attr moto123
group-attr group1 group-filter "groupfilter1" group-membership
groupmembership1 net-timeout 2
 session-resumption lifetime 10 max-entries 11
rfs7000-37FABE(config-radius-server-policy-test)#
```

Related Commands:

no	Disables session resumption on this RADIUS server policy

use

radius-server-policy

Defines settings used with the RADIUS server policy

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
use [radius-group <RAD-GROUP-NAME1> {RAD-GROUP-NAME2}|radius-user-pool-policy
          <RAD-USER-POOL-NAME>]
```

Parameters

```
use [radius-group <RAD-GROUP-NAME1> {RAD-GROUP-NAME2}|radius-user-pool-policy
<RAD-USER-POOL-NAME>]
```

radius-group <RAD-GROUP-NAME1> {RAD-GROUP-NAME2}	Associates a specified RADIUS group (for LDAP users) with this RADIUS server policy You can optionally associate two RADIUS groups with one RADIUS server policy.
radius-user-pool-policy <RAD-USER-POOL-NAME>	Associates a specified RADIUS user pool with this RADIUS server policy. Specify a user pool name.

Example

```
rfs7000-37FABE(config-radius-server-policy-test)#use radius-group test

rfs7000-37FABE(config-radius-server-policy-test)#show context
radius-server-policy test
 proxy retry-delay 8
 proxy retry-count 4
 proxy realm test1 server 172.16.10.7 port 1025 secret 0 motorolaSol1123
 ldap-server primary host 172.16.10.19 port 162 login "motorolasol" bind-dn
"bind-dn1" base-dn "bas-dn1" passwd 0 motorolasol@123 passwd-attr moto123
group-attr group1 group-filter "groupfilter1" group-membership
groupmembership1 net-timeout 2
 use radius-group test
 session-resumption lifetime 10 max-entries 11
rfs7000-37FABE(config-radius-server-policy-test)#
```

Related Commands:

no	Disassociates a RADIUS group or a RADIUS user pool policy from this RADIUS server policy

radius-user-pool-policy

RADIUS-POLICY

Configures a RADIUS user pool policy

A user pool defines policies for individual user access to the internal RADIUS resources. User pool policies define unique permissions (either temporary or permanent) that control user access to the local RADIUS resources. A pool can contain a single user or multiple users.

Use the (config) instance to configure RADIUS user pool policy commands. To navigate to the radius-user-pool-policy instance, use the following commands:

```
<DEVICE>(config)#radius-user-pool-policy <POOL-NAME>

rfs7000-37FABE(config)#radius-user-pool-policy testuser
rfs7000-37FABE(config-radius-user-pool-testuser)#
```

The following table summarizes RADIUS user pool policy configuration commands.

Commands	Description	Reference
user	Configures the RADIUS user parameters	page 1069
no	Negates a command or sets its default	page 1069
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

user

radius-user-pool-policy

Configures RADIUS user parameters

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
user <USERNAME> password [0 <UNECRYPTED-PASSWORD>|2
<ECRYPTED-PASSWORD>|<PASSWORD>]
          {group <RAD-GROUP> {<RAD-GROUP>|guest}}

user <USERNAME> password [0 <UNECRYPTED-PASSWORD>|2
<ECRYPTED-PASSWORD>|<PASSWORD>]
          {group <RAD-GROUP> {guest expiry-time <HH:MM> expiry-date
<MM:DD:YYYY>
          {(email-id <EMAIL-ID>|start-time <HH:MM> start-date <MM:DD:YYY>|
          telephone <TELEPHONE-NUMBER>)}}}
```

Parameters

```
user <USERNAME> password [0 <UNECRYPTED-PASSWORD>|2
<ECRYPTED-PASSWORD>|<PASSWORD>]
{group <RAD-GROUP> {guest expiry-time <HH:MM> expiry-date <MM:DD:YYY>
{(email-id <EMAIL-ID>|start-time <HH:MM> start-date <MM:DD:YYY>|
telephone <TELEPHONE-NUMBER>)}}}
```

user <USERNAME>	Adds a new RADIUS user to the RADIUS user pool • <USERNAME> – Specify the name of the user. The username should not exceed 64 characters. **NOTE:** The username is a unique alphanumeric string identifying this user, and cannot be modified with the rest of the configuration.
passwd [0 <UNENCRYPTED-PASSWORD> | 2 <ENCRYPTED-PASSWORD>| <PASSWORD>]	Configures the user password (provide a password unique to this user) • 0 <UNENCRYPTED-PASSWORD> – Sets an unencrypted password • 2 <ENCRYPTED-PASSWORD> – Sets an encrypted password • <PASSWORD> – Sets a password (specified unencrypted) up to 21 characters
group <RAD-GROUP>	Optional. Configures the RADIUS server group of which this user is a member • <RAD-GROUP> – Specify a group name in the local database. If the user is a guest, assign the user a group with temporary access privileges.
guest	Optional. Specifies that this user is a guest user. Guest users have restricted access. After enabling a guest user account, specify the start and expiry time and date for this account. A guest user can be assigned only to a guest user group.
expiry-time <HH:MM>	Optional. Specify the user account expiry time in the HH:MM format (for example, 12:30 means 30 minutes after 12:00 the user login will expire).
expiry-date <MM:DD:YYYY>	Optional. Specify the user account expiry date in the MM:DD:YYYY format (for example. 02:15:2013).
start-time <HH:MM>	Optional. Specify the user account activation time in the HH:MM format.
start-date <MM:DD:YYYY>	Optional. Specify the user account activation date in the MM:DD:YYYY format.
(email-id <EMAIL-ID>| start-time <HH:MM> start-date <MM:DD:YYY>| telephone <TELEPHONE-NUMBER>)	After configuring the above user details, optionally configure the following user information: • email-id – User's e-mail ID • start-time – User's account activation time • telephone – User's telephone number (should include the area code)

Example

```
rfs7000-37FABE(config-radius-user-pool-testuser)#user testuser password 0
motorolasol@123 group test1 guest expiry-time 13:20 expiry-date 12:25:2013
start-time
17:00 start-date 01:05:2013
rfs7000-37FABE(config-radius-user-pool-testuser)#

rfs7000-37FABE(config-radius-user-pool-testuser)#show context
radius-user-pool-policy testuser
 user testuser password 0 motorolasol@123 group test1 guest expiry-time 13:20
expiry-date 12:25:2013 start-time 17:00 start-date 01:05:2013
rfs7000-37FABE(config-radius-user-pool-testuser)#
```

Related Commands:

no	Deletes a user from a RADIUS user pool

no

radius-user-pool-policy

Negates a command or sets its default. When used in the RADIUS user pool policy mode, the no command deletes a user from a RADIUS user pool

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no user <USERNAME>
```

Parameters

```
no user <USERNAME>
```

user <USERNAME>	Deletes a RADIUS user • <USERNAME> – Specify the user name.

Example

```
The following example shows the RADIUS user pool ‘testuser’ settings before
the ‘no’ command is executed:

rfs7000-37FABE(config-radius-user-pool-testuser)#show context
radius-user-pool-policy testuser
 user testuser password 0 motorolasol@123 group test1 guest expiry-time 13:20
expiry-date 12:25:2013 start-time 17:00 start-date 01:05:2013
rfs7000-37FABE(config-radius-user-pool-testuser)#

rfs7000-37FABE(config-radius-user-pool-testuser)#no user testuser

The following example shows the RADIUS user pool ‘testuser’ settings after the
‘no’ command is executed:

rfs7000-37FABE(config-radius-user-pool-testuser)#show context
radius-user-pool-policy testuser
rfs7000-37FABE(config-radius-user-pool-testuser)#
```

Related Commands:

user	Configures the RADIUS user parameters

Chapter

RADIO-QOS-POLICY

18

This chapter summarizes the radio QoS policy in the CLI command structure.

Configuring and implementing a radio QoS policy is essential for WLANs with heavy traffic and less bandwidth. The policy enables you to provide preferential service to selected network traffic by controlling bandwidth allocation. The radio QoS policy can be applied to VLANs configured on an access point. In case no VLANs are configured, the radio QoS policy can be applied to an access point's Ethernet and radio ports.

Without a dedicated QoS policy, a network operates on a best-effort delivery basis, meaning all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped!

When configuring a QoS policy for a radio, select specific network traffic, prioritize it, and use congestion-management and congestion-avoidance techniques to provide deployment customizations best suited to each QoS policy's intended wireless client base.

A well designed QoS policy should:

- Classify and mark data traffic to accurately prioritize and segregate it (by access category) throughout the network.
- Minimize network delay and jitter for latency sensitive traffic.
- Ensure higher priority traffic has a better likelihood of delivery in the event of network congestion.
- Prevent ineffective utilization of access points degrading session quality by configuring admission control mechanisms within each radio QoS policy.

Within a Brocade wireless network, wireless clients supporting low and high priority traffic contend with one another for access and data resources. The IEEE 802.11e amendment has defined *Enhanced Distributed Channel Access* (EDCA) mechanisms stating high priority traffic can access the network sooner then lower priority traffic. The EDCA defines four traffic classes (or access categories); voice (highest), video (next highest), best effort, and background (lowest). The EDCA has defined a time interval for each traffic class, known as the *Transmit Opportunity* (TXOP). The TXOP prevents traffic of a higher priority from completely dominating the wireless medium, thus ensuring lower priority traffic is still supported.

IEEE 802.11e includes an advanced power saving technique called *Unscheduled Automatic Power Save Delivery* (U-APSD) that provides a mechanism for wireless clients to retrieve packets buffered by an access point. U-APSD reduces the amount of signaling frames sent from a client to retrieve buffered data from an access point. U-APSD also allows access points to deliver buffered data frames as *bursts*, without backing-off between data frames. These improvements are useful for voice clients, as they provide improved battery life and call quality.

The Wi-Fi alliance has created *Wireless Multimedia* (WMM) and *WMM Power Save* (WMM-PS) certification programs to ensure interoperability between 802.11e WLAN infrastructure implementations and wireless clients. A Brocade wireless network supports both WMM and WMM-Power Save techniques. WMM and WMM-PS (U-APSD) are enabled by default in each WLAN profile.

Enabling WMM support on a WLAN just advertises the WLAN's WMM capability and radio configuration to wireless clients. The wireless clients must also support WMM and use the values correctly while accessing the WLAN to benefit.

WMM includes advanced parameters (CWMin, CWMax, AIFSN and TXOP) specifying back-off duration and inter-frame spacing when accessing the network. These parameters are relevant to both connected access point radios and their wireless clients. Parameters impacting access point transmissions to their clients are controlled using per radio WMM settings, while parameters used by wireless clients are controlled by a WLAN's WMM settings.

Brocade controllers (access points, wireless controllers, and service platforms) include a *Session Initiation Protocol* (SIP), *Skinny Call Control Protocol* (SCCP) and *Application Layer Gateway* (ALG) enabling devices to identify voice streams and dynamically set voice call bandwidth.

Brocade controllers support static QoS mechanisms per WLAN to provide prioritization of WLAN traffic when legacy (non WMM) clients are deployed. When enabled on a WLAN, traffic forwarded to a client is prioritized and forwarded based on the WLAN's WMM access control setting.

NOTE
Statically setting a WLAN WMM access category value only prioritizes traffic to the client.

Wireless network administrators can also assign weights to each WLAN in relation to user priority levels. The lower the weight, the lower the priority. Use a weighted technique to achieve different QoS levels across WLANs.

Brocade devices rate-limit bandwidth for WLAN sessions. This form of per-user rate limiting enables administrators to define uplink and downlink bandwidth limits for users and clients. This sets the level of traffic a user or client can forward and receive over the WLAN. If the user or client exceeds the limit, excessive traffic is dropped.

Rate limits can be applied to WLANs using groups defined locally or externally from a RADIUS server using Brocade *Vendor Specific Attributes* (VSAs). Rate limits can be applied to users authenticating using 802.1X, captive portal authentication, and devices using MAC authentication.

Use the (config) instance to configure radios QoS policy related configuration commands. To navigate to the
radio QoS policy instance, use the following commands:

```
<DEVICE>(config)#radio-qos-policy <POLICY-NAME>

rfs7000-37FABE(config)#radio-qos-policy test
rfs7000-37FABE(config-radio-qos-test)#?
Radio QoS Mode commands:
  accelerated-multicast  Configure multicast streams for acceleration
  admission-control      Configure admission-control on this radio for one or
                         more access categories
  no                     Negate a command or set its defaults
  smart-aggregation      Configure smart aggregation parameters
  wmm                    Configure 802.11e/Wireless MultiMedia parameters

  clrscr                 Clears the display screen
  commit                 Commit all changes made in this session
  do                     Run commands from Exec mode
  end                    End current mode and change to EXEC mode
  exit                   End current mode and down to previous mode
  help                   Description of the interactive help system
  revert                 Revert changes
  service                Service Commands
  show                   Show running system information
```

```
  write                  Write running configuration to memory or terminal

rfs7000-37FABE(config-radio-qos-test)#
```

radio-qos-policy

Table 16 summarizes radio QoS policy configuration commands.

TABLE 16 Radio-QoS-Policy-Config Commands

Command	Description	Reference
accelerated-multicast	Configures multicast streams for acceleration	page 1073
admission-control	Enables admission control across all radios for one or more access categories	page 1074
no	Negates a command or resets configured settings to their default	page 1077
smart-aggregation	Configures smart aggregation parameters	page 1080
service	Invokes service commands in the radio QoS configuration mode	page 1082
wmm	Configures 802.11e/wireless multimedia parameters	page 1083
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
show	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

accelerated-multicast

radio-qos-policy

Configures multicast streams for acceleration. Multicasting allows group transmission of data streams.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
accelerated-multicast
[client-timeout|max-client-streams|max-streams|overflow-policy|
          stream-threshold]

accelerated-multicast [client-timeout <5-6000>|max-client-streams <1-4>|
          max-streams <0-256>|overflow-policy
[reject|revert]|stream-threshold <1-500>]
```

Parameters

```
accelerated-multicast [client-timeout <5-6000>|max-client-streams <1-4>|
max-streams <0-256>|overflow-policy [reject|revert]|stream-threshold <1-500>]
```

client-timeout <5-6000>	Configures a timeout period in seconds for wireless clients • <5-6000> – Specify a value from 5 - 6000 seconds. The default is 60 seconds.
max-client-streams <1-4>	Configures the maximum number of accelerated multicast streams per client • <1-4> – Specify a value from 1 - 4. The default is 2.
max-streams <0-256>	Configures the maximum number of accelerated multicast streams per radio • <0-256> – Specify a value from 0 - 256. The default is 25.
overflow-policy [reject|revert]	Specifies the policy in case too many clients register simultaneously. The radio QOS policy can be configured to follow one of the following courses of action: • reject – Rejects new clients. The default overflow policy is reject. • revert – Reverts to regular multicast delivery When the number of wireless clients using accelerated multicast exceeds the configured value (max-streams), the radio can either reject new wireless clients or revert existing clients to a non-accelerated state.
stream-threshold <1-500>	Configures the number of multicast packets per second threshold value. Once this threshold is crossed, the system triggers streams to accelerate. • <1-500> – Specify a value from 1 - 500. The default is 25 packets per second.

Example

```
rfs7000-37FABE(config-radio-qos-test)#accelerated-multicast client-timeout
500
rfs7000-37FABE(config-radio-qos-test)#accelerated-multicast stream-threshold
15

rfs7000-37FABE(config-radio-qos-test)#show context
radio-qos-policy test
 accelerated-multicast stream-threshold 15
 accelerated-multicast client-timeout 500
rfs7000-37FABE(config-radio-qos-test)#
```

Related Commands:

no	Reverts accelerated multicasting settings to their default

admission-control

radio-qos-policy

Enables admission control across all radios for one or more access categories. Enabling admission control for an access category, ensures clients associated to an access point and complete WMM admission control before using that access category.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
admission-control
[background|best-effort|firewall-detected-traffic|implicit-tspec|
          video|voice]

admission-control [firewall-detected-traffic|implicit-tspec]

admission-control [background|best-effort|video|voice] {max-airtime-percent|
          max-clients|max-roamed-clients|reserved-for-roam-percent}

admission-control [background|best-effort|video|voice] {max-airtime-percent
<0-150>|
          max-clients <0-256>|max-roamed-clients
<0-256>|reserved-for-roam-percent <0-150>}
```

Parameters

```
admission-control [firewall-detected-traffic|implicit-tspec]
```

admission-control firewall-detected-traffic	Enforces admission control for traffic whose access category is detected by the firewall ALG. For example, SIP voice calls. This feature is enabled by default. When enabled, the firewall simulates reception of frames for voice traffic when the voice traffic was originated via SIP or SCCP control traffic. If a client exceeds configured values, the call is stopped and/or received voice frames are forwarded at the next non admission controlled traffic class priority. This applies to clients that do not send TPSEC frames only.
admission-control implicit-tspec	Enables implicit traffic specifiers for clients that do not support WMM TSPEC, but are accessing admission-controlled access categories. This feature is enabled by default. This feature requires wireless clients to send their traffic specifications to an access point before they can transmit or receive data. If enabled, this setting applies to this radio QoS policy. When enabled, the access point simulates the reception of frames for any traffic class by looking at the amount of traffic the client is receiving and sending. If the client sends more traffic than has been configured for an admission controlled traffic class, the traffic is forwarded at the priority of the next non admission controlled traffic class. This applies to clients that do not send TPSEC frames only.

```
admission-control [background|best-effort|video|voice]
{max-airtime-percent <0-150>|max-clients <0-256>|max-roamed-clients <0-256>|
reserved-for-roam-percent <0-150>}
```

admission-control background	Configures background access category admission control parameters
admission-control best-effort	Configures best effort access category admission control parameters
admission-control video	Configures video access category admission control parameters
admission-control voice	Configures voice access category admission control parameters

max-airtime-percent <0-150>	Optional. Specifies the maximum percentage of airtime, including oversubscription, for the following access category: • background – Sets the maximum airtime (in the form of a percentage of the radio's bandwidth) allotted to admission control for low (background) client traffic. Background traffic only needs a short radio airtime to process, so set an intermediate airtime value if this radio QoS policy is reserved to support background data. • best-effort – Sets the maximum airtime (in the form of a percentage of the radio's bandwidth) allotted to admission control for normal (best-effort) client traffic. Normal best effort traffic needs a short radio airtime to process, so set an intermediate airtime value if this radio QoS policy is reserved for best effort data support. • video – Sets the maximum airtime (in the form of a percentage of the radio's bandwidth) allotted to admission control for voice supported client traffic. Video traffic requires longer radio airtime to process, so set a longer airtime value if this radio QoS policy is intended to support video. • voice – Sets the maximum airtime (in the form of a percentage of the radio's bandwidth) allotted to admission control for voice supported client traffic. Voice traffic requires longer radio airtime to process, so set a longer airtime value if this radio QoS policy is intended to support voice. The following keyword is common to all of the above traffic types: • <0-150> – Specify a value from 0 - 150. This is the maximum percentage of airtime, including oversubscription, for the selected access category. The default is 75%.
max-clients <0-256>	Optional. Specifies the maximum number of wireless clients admitted to the following access categories: • background – Sets the number of wireless clients supporting low (background) traffic allowed to exist (and consume bandwidth) within the radio's QoS policy • best-effort – Sets the number of wireless clients supporting normal (best-effort) traffic allowed to exist (and consume bandwidth) within the radio's QoS policy • video – Sets the number of video supported wireless clients allowed to exist (and consume bandwidth) within the radio's QoS policy. • voice – Sets the number of voice supported wireless clients allowed to exist (and consume bandwidth) within the radio's QoS policy. Since voice and video supported wireless clients use a greater portion of a controller's resources than lower bandwidth traffic (like low and best effort categories), consider setting the max-client value proportionally to the number of other QoS policies supporting voice access category clients. The following keyword is common to all of the above traffic types: • <0-256> – Specify a value from 0 - 256. This is the maximum number of wireless clients admitted to the selected access category. The default is 100 clients.

max-roamed-clients <0-256>	Optional. Specifies the maximum number of roaming wireless clients admitted to the selected access category • background – Sets the number of low (background) supported wireless clients allowed to roam to a different access point radio • best-effort – Sets the number of normal (best-effort) supported wireless clients allowed to roam to a different access point radio • video – Sets the number of video supported wireless clients allowed to roam to a different access point radio • voice – Sets the number of voice supported wireless clients allowed to roam to a different access point radio The following keyword is common to all of the above traffic types: • <0-256> – Specify a value from 0 - 256. This is the maximum number of roaming wireless clients admitted to the selected access category. The default is 10 roamed clients.
reserved-for-roam-percent <0-150>	Optional. Calculates the percentage of air time, including oversubscription, allocated exclusively for roaming clients. This value is calculated relative to the configured max air time for this access category. • background – Sets the roam utilization (in the form of a percentage of the radio's bandwidth) allotted to admission control for low (background) supported clients who have roamed to a different radio. • best-effort – Sets the roam utilization (in the form of a percentage of the radio's bandwidth) allotted to admission control for normal (best-effort) supported clients who have roamed to a different radio. • video – Sets the roam utilization (in the form of a percentage of the radio's bandwidth) allotted to admission control for video supported clients who have roamed to a different radio. • voice – Sets the roam utilization (in the form of a percentage of the radio's bandwidth) allotted to admission control for voice supported clients who have roamed to a different radio. The following keyword is common to all of the above traffic types: • <0-150> – Specify a value from 0 - 150. This is the percentage of air time, including oversubscription, allocated exclusively for roaming clients associated with the selected access category. The default is 10%.

Example

```
rfs7000-37FABE(config-radio-qos-test)#admission-control best-effort
max-clients 200
rfs7000-37FABE(config-radio-qos-test)#admission-control voice
reserved-for-roam-percent 8
rfs7000-37FABE(config-radio-qos-test)#admission-control voice
max-airtime-percent 9

rfs7000-37FABE(config-radio-qos-test)#show context
radio-qos-policy test
 admission-control voice max-airtime-percent 9
 admission-control voice reserved-for-roam-percent 8
 admission-control best-effort max-clients 200
 accelerated-multicast stream-threshold 15
 accelerated-multicast client-timeout 500
rfs7000-37FABE(config-radio-qos-test)#
```

Related Commands:

no	Reverts or resets admission control settings to their default

no

radio-qos-policy

Negates a command or resets configured settings to their default. When used in the radio QOS policy mode, the no command enables the resetting of accelerated multicast parameters, admission control parameters, and MultiMedia parameters.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no [accelerated-multicast|admission-control|smart-aggregation|wmm|service]

no accelerated-multicast [client-timeout|max-client-streams|max-streams|
        overflow-policy|stream-threshold]

no admission-control [firewall-detected-traffic|implicit-tspec|background|
        best-effort|video|voice]
no admission-control [firewall-detected-traffic|implicit-tspec]
no admission-control [background|best-effort|video|voice]
{max-airtime-percent|
        max-clients|max-roamed-clients|reserved-for-roam-percent}

no smart-aggregation {delay|max-mesh-hops|min-aggregation-limit}
no smart-aggregation {delay [background|best-effort|streaming-video|
        video-conferencing|voice]|max-mesh-hops|min-aggregation-limit}

no wmm [background|best-effort|video|voice] [aifsn|cw-max|cw-min|txop-limit]

no service admission-control across-reassoc
```

Parameters

```
no accelerated-multicast [client-timeout|max-client-streams|max-streams|
overflow-policy|stream-threshold]
```

no accelerated-multicast	Resets accelerated multicasting settings to their default. The following accelerated multicast control settings can be reverted: • client-timeout – Resets the client timeout to the default (60 seconds) • max-client-streams – Resets the maximum number of accelerated streams per client to default (2 streams per client) • max-streams – Resets the maximum number of accelerated streams per radio to default (25 streams) • overflow-policy – Resets the overflow policy to default (reject) • stream-threshold – Resets the number of packets per second threshold to default (25 packets)

```
no admission-control [firewall-detected-traffic|implicit-tspec]
```

no admission-control	Reverts or resets admission control settings to their default. These controls are configured on a radio for one or more access categories. • firewall-detected-traffic – Does not enforce admission control for traffic whose access category is detected by the firewall ALG • implicit-tspec – Disables implicit traffic specifiers for wireless clients that do not support WMM-TSPEC

`no admission-control [background|best-effort|video|voice] {max-airtime-percent| max-clients|max-roamed-clients|reserved-for-roam-percent}`

no admission-control	Reverts or resets admission control settings to their default. These controls are configured on a radio for one or more access categories. • background – Resets background access category admission control settings • best-effort – Resets best effort access category admission control settings • video – Resets video access category admission control settings • voice – Resets voice access category admission control settings
max-airtime-percent	Optional. Resets the maximum percentage of airtime used by the selected access category to its default (75%)
max-clients	Optional. Resets the maximum number of wireless clients admitted by the selected access category to its default (100 clients)
max-roamed-clients	Optional. Resets the maximum number of roaming wireless clients admitted by the selected access category to its default (10 roamed clients)
reserved-for-roam-percent	Resets the percentage of air time allocated exclusively for roaming wireless clients by the selected access category to its default (10%)

`no smart-aggregation {delay [background|best-effort|streaming-video| video-conferencing|voice]|max-mesh-hops|min-aggregation-limit}`

no smart-aggregation	Disable smart aggregation parameters
delay [background|best-effort| streaming-video| video-conferencing|voice]	Optional. Removes the configured maximum delay setting for the specified traffic type
max-mesh-hops	Optional. Removes the configured maximum number of expected mesh hops
min-aggregation-limit	Optional. Removes the minimum number of aggregates buffered before an aggregate is sent

`no wmm [background|best-effort|video|voice] [aifsn|cw-max|cw-min|txop-limit]`

no wmm	Reverts or resets 802.11e/wireless multimedia settings to default • background – Removes background access category wireless multimedia settings • best-effort – Removes best effort access category wireless multimedia settings • video – Removes video access category wireless multimedia settings • voice – Removes voice access category wireless multimedia settings The following are common to the background, best-effort, video, and voice parameters:
aifsn	Removes the configured AIFSN value
cw-max	Removes the configured maximum contention window value
cw-min	Removes the configured minimum contention window value
txop-limit	Removes the configured transmit opportunity limit value

`no service admission-control across-reassoc`

no service admission-control across-reassoc	Disables retention of previously negotiated TSPEC parameters across re-associations on the radio

Example

```
The following example shows the Radio-qos-policy ‘test’ settings before the
‘no’ commands are executed:
```

```
rfs7000-37FABE(config-radio-qos-test)#show context
radio-qos-policy test
 admission-control voice max-airtime-percent 9
 admission-control voice reserved-for-roam-percent 8
 admission-control best-effort max-clients 200
 accelerated-multicast stream-threshold 15
 accelerated-multicast client-timeout 500
rfs7000-37FABE(config-radio-qos-test)#

rfs7000-37FABE(config-radio-qos-test)#no admission-control best-effort
max-clients
rfs7000-37FABE(config-radio-qos-test)#no accelerated-multicast client-timeout

The following example shows the Radio-qos-policy 'test' settings after the
'no' commands are executed:

rfs7000-37FABE(config-radio-qos-test)#show context
radio-qos-policy test
 admission-control voice max-airtime-percent 9
 admission-control voice reserved-for-roam-percent 8
 accelerated-multicast stream-threshold 15
rfs7000-37FABE(config-radio-qos-test)#

rfs4000-229D58(config-radio-qos-test)#show context
radio-qos-policy test
 service admission-control across-reassoc
rfs4000-229D58(config-radio-qos-test)#

rfs4000-229D58(config-radio-qos-test)#no service admission-control
across-reassoc

rfs4000-229D58(config-radio-qos-test)#show context
radio-qos-policy test
rfs4000-229D58(config-radio-qos-test)#
```

Related Commands:

accelerated-multicast	Configures multicast streams for acceleration. Multicasting allows the group transmission of data streams
admission-control	Enables admission control across all radios for one or more access categories
smart-aggregation	Configures smart aggregation parameters on this Radio QoS policy
service	Invokes service commands in the radio QoS configuration mode
wmm	Configures 802.11e wireless multimedia parameters

smart-aggregation

radio-qos-policy

Configures smart aggregation parameters on this Radio QoS policy

Smart aggregation enhances frame aggregation by dynamically selecting the time when the aggregated frame is transmitted. In a frame's typical aggregation, an aggregated frame is sent when:

- A pre-configured number of aggregated frames is reached

- An administrator-defined interval has elapsed since the first frame (of a set of frames to be aggregated) was received
- An administrator-defined interval has elapsed since the last frame (not necessarily the final frame) of a set of frames to be aggregated was received

With this enhancement, an aggregation delay is set uniquely for each traffic class. For example, voice traffic might not be aggregated, but sent immediately. Whereas, background data traffic is set a delay for aggregating frames, and these aggregated frames are sent.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
smart-aggregation {delay|max-mesh-hops|min-aggregation-limit}

smart-aggregation {delay
[background|best-effort|streaming-video|video-conferencing|
          voice] <0-1000>}

smart-aggregation {max-mesh-hops <1-10>}

smart-aggregation {min-aggregation-limit <0-64>}
```

Parameters

```
smart-aggregation {delay
[background|best-effort|streaming-video|video-conferencing|
voice] <0-1000>}
```

delay	Optional. Configures the maximum delay parameter for each traffic type This is the maximum delay, in milliseconds, in the transmission of the first frame received.
background	Configures the maximum delay parameter, in milliseconds, for background traffic (250 msec)
best-effort	Configures the maximum delay parameter, in milliseconds, for best effort traffic (150 msec)
streaming-video	Configures the maximum delay parameter, in milliseconds, for streaming video traffic (150 msec)
video-conferencing	Configures the maximum delay parameter, in milliseconds, for video conference traffic (40 msec)
voice	Configures the maximum delay parameter, in milliseconds, for voice traffic (0 msec)
<0-1000>	This parameter is common to all of the above traffic types. • <0-1000> – Specify a value from 0 - 1000 msec.

```
smart-aggregation {max-mesh-hops <1-10>}
```

max-mesh-hops <1-10>	Optional. Sets the maximum number of expected hops to the destination within a mesh • <1-10> – Specify a value from 1 - 10. The default is 3 hops.

```
smart-aggregation {min-aggregation-limit <0-64>}
```

min-aggregation-limit <0-64>	Optional. Sets the minimum number of aggregates buffered before an aggregate is sent • <0-64> – Specify a value from 0 - 64. The default is 8 frames.

Example

```
rfs7000-37FABE(config-radio-qos-test)#smart-aggregation delay voice 50

rfs7000-37FABE(config-radio-qos-test)#smart-aggregation delay background 100

rfs7000-37FABE(config-radio-qos-test)#show context
radio-qos-policy test
 smart-aggregation delay voice 50
 smart-aggregation delay background 100
rfs7000-37FABE(config-radio-qos-test)#
```

Related Commands:

no	Resets the minimum aggregation limit

service

radio-qos-policy

Invokes service commands in the radio QoS configuration mode

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
service [admission-control|show]

service admission-control across-reassoc

service show cli
```

Parameters

```
service admission-control across-reassoc
```

service	Invokes service commands
admission-control across-reassoc	Retains previously negotiated TSPEC parameters across re-associations on the radio For more information on admission-control parameters, see *admission-control*.

```
service show cli
```

service show cli	Displays running system information • cli – Displays the Radio QoS mode's CLI tree

Example

```
rfs4000-229D58(config-radio-qos-test)#service admission-control
across-reassoc
rfs4000-229D58(config-radio-qos-test)#

rfs4000-229D58(config-radio-qos-test)#show context
radio-qos-policy test
 service admission-control across-reassoc
rfs4000-229D58(config-radio-qos-test)#

rfs4000-229D58(config-radio-qos-test)#service show cli
Radio QoS Mode mode:
+-help [help]
  +-search
    +-WORD [help search WORD (|detailed|only-show|skip-show|skip-no)]
      +-detailed [help search WORD (|detailed|only-show|skip-show|skip-no)]
      +-only-show [help search WORD (|detailed|only-show|skip-show|skip-no)]
      +-skip-show [help search WORD (|detailed|only-show|skip-show|skip-no)]
      +-skip-no [help search WORD (|detailed|only-show|skip-show|skip-no)]
+-show
  +-commands [show commands]
  +-adoption
    +-log
      +-adoptee [show adoption log adoptee(|on DEVICE-NAME)]
        +-on
          +-DEVICE-NAME [show adoption log adoptee(|on DEVICE-NAME)]
      +-adopter [show adoption log adopter (|mac AA-BB-CC-DD-EE-FF)(|on
DEVICE-NAME)]
        +-mac
          +-AA-BB-CC-DD-EE-FF [show adoption log adopter (|mac
AA-BB-CC-DD-EE-FF)(|on DEVICE-NAME)]
            +-on
              +-DEVICE-NAME [show adoption log adopter (|mac
AA-BB-CC-DD-EE-FF)(|on DEVICE-NAME)]
--More--
```

Related Commands:

no	Disables retention of previously negotiated TSPEC parameters across re-associations on the radio

wmm

radio-qos-policy

Configures 802.11e *wireless multimedia* (wmm) parameters

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
wmm [background|best-effort|video|voice]

wmm [background|best-effort|video|voice] [aifsn <1-15>|cw-max <0-15>|cw-min
<0-15>|
          txop-limit <0-65535>]
```

Parameters

```
wmm [background|best-effort|video|voice] [aifsn <1-15>|cw-max <0-15>|cw-min
<0-15>|
txop-limit <0-65535>]
```

wmm background	Configures background access category wireless multimedia settings
wmm best-effort	Configures best effort access category wireless multimedia settings
wmm video	Configures video access category wireless multimedia settings
wmm voice	Configures voice access category wireless multimedia settings
aifsn <1-15>	Configures *Arbitrary Inter-Frame Space Number* (AIFSN) as the wait time between data frames derived from the AIFSN and slot time • background – Sets the current AIFSN for low (background) traffic. The default is 7. • best-effort – Sets the current AIFSN for normal (best-effort) traffic. The default is 3. • video – Set the current AIFSN for video traffic. Higher-priority traffic video categories should have lower AIFSNs than lower-priority traffic categories. This causes lower-priority traffic to wait longer before attempting access. The default is 1. • voice – Sets the current AIFSN for voice traffic. Higher-priority traffic voice categories should have lower AIFSNs than lower-priority traffic categories. This causes lower-priority traffic to wait longer before attempting access. The default is 1. The following keyword is common to all of the above traffic types: • <1-15> – Sets a value from 1 - 15
cw-max <0-15>	Clients pick a number between 0 and the min contention window to wait before retransmission. Clients then double their wait time on a collision, until it reaches the maximum contention window. • background – Sets CW Max for low (background) traffic. The default is 10. • best-effort – Sets CW Max for normal (best effort) traffic. The default is 6. • voice – Sets CW Max for voice traffic. The default is 3. • video – Sets CW Max for video traffic. The default is 4 The following keyword is common to all of the above traffic types: • <0-15> – ECW: the contention window. The actual value used is (2^ECW - 1). **NOTE:** Lower values are used for higher priority traffic (like video and voice) and higher values are used for lower priority traffic (like background and best-effort).

cw-min <0-15>	Clients select a number between 0 and the min contention window to wait before retransmission. Clients then double their wait time on a collision, until it reaches the maximum contention window. • background – Sets CW Min for low (background) traffic. The default is 4. • best-effort – Sets CW Min for normal (best effort) traffic. The default is 4. • voice – Sets CW Min for voice traffic. The default is 2. • video – Sets CW Min for video traffic. The default is 3. The following keyword is common to all of the above traffic types: • <0-15> – ECW: the contention window. The actual value used is (2^ECW - 1). **NOTE:** Lower values are used for higher priority traffic (like video and voice) and higher values are used for lower priority traffic (like background and best-effort).
txop-limit <0-65535>	Set the interval, in microseconds, during which a particular client has the right to initiate transmissions • background – Sets TXOP for low (background) traffic. The default is 0. • best-effort – Sets TXOP for normal (best effort) traffic. The default is 4. • voice – Sets TXOP for voice traffic. The default is 47. • video – Sets TXOP for video traffic. The default is 94. The following keyword is common to all of the above traffic types: • <0-65535> – Specify a value from 0 - 65535 to configure the transmit opportunity limit in 32 microsecond units. **NOTE:** Lower values are used for higher priority traffic (like video and voice) and higher values are used for lower priority traffic (like background and best-effort).

Usage Guidelines:

Before defining a radio QoS policy, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- To support QoS, each multimedia application, wireless client, and WLAN is required to support WMM.
- WMM enabled clients can co-exist with non-WMM clients on the same WLAN. Non-WMM clients are always assigned a Best Effort access category.
- Brocade recommends default WMM values be used for all deployments. Changing these values can lead to unexpected traffic blockages, and the blockages might be difficult to diagnose.
- Overloading an access point radio with too much high priority traffic (especially voice) degrades overall service quality for all users.
- TSPEC admission control is only available with newer voice over WLAN phones. Many legacy voice devices do not support TPSEC or even support WMM traffic prioritization.

Example

```
rfs7000-37FABE(config-radio-qos-test)#wmm best-effort aifsn 7
rfs7000-37FABE(config-radio-qos-test)#wmm voice txop-limit 1

rfs7000-37FABE(config-radio-qos-test)#show context
radio-qos-policy test
 wmm best-effort aifsn 7
 wmm voice txop-limit 1
 admission-control voice max-airtime-percent 9
 admission-control voice reserved-for-roam-percent 8
 accelerated-multicast stream-threshold 15
rfs7000-37FABE(config-radio-qos-test)#
```

Related Commands:

no	Reverts or resets 802.11e/wireless multimedia settings to their default

Chapter

ROLE-POLICY 19

This chapter summarizes the role policy commands in the CLI command structure.

A well defined role policy simplifies user management, and is a significant aspect of WLAN management. It acts as a role based firewall (much like ACLs) consisting of user-defined roles. Each role has a set of match criteria (filters) used to filter wireless clients. The action taken when a client matches the defined filters, is determined by the IP or MAC ACL associated with the user-defined role. Based on the conditions specified in the IP and/or MAC ACL, clients are granted or denied access to the controller managed network. The role policy also defines the VLAN and data rates assigned to clients provided network access.

A role policy also enables LDAP service, allowing controllers and access points to retrieve user information from the LDAP server. This information is matched with the user-defined role filters to determine if a client matches the role or not, and should be allowed or denied access to the controller managed network.

Use the (config-role-policy) instance to configure role policy related configuration commands. To navigate to the
config-role instance, use the following commands:

```
<DEVICE>(config)#role-policy <POLICY-NAME>

rfs7000-37FABE(config)#role-policy test
rfs7000-37FABE(config-role-policy-test)#?
Role Policy Mode commands:
  default-role     Configuration for Wireless Clients not matching any role
  ldap-deadperiod  Ldap dead period interval
  ldap-query       Set the ldap query mode
  ldap-server      Add a ldap server
  ldap-timeout     Ldap query timeout interval
  no               Negate a command or set its defaults
  user-role        Create a role

  clrscr           Clears the display screen
  commit           Commit all changes made in this session
  do               Run commands from Exec mode
  end              End current mode and change to EXEC mode
  exit             End current mode and down to previous mode
  help             Description of the interactive help system
  revert           Revert changes
  service          Service Commands
  show             Show running system information
  write            Write running configuration to memory or terminal

rfs7000-37FABE(config-role-policy-test)#
```

role-policy

ROLE-POLICY

Table 17 summarizes role policy configuration commands.

TABLE 17 Role-Policy-Config Commands

Command	Description	Reference
default-role	Assigns the default role to clients not matching any of the user-defined roles defined in the role policy	page 1088
ldap-deadperiod	Configures the *Lightweight Directory Access Protocol* (LDAP) deadperiod interval	page 1089
ldap-query	Enables LDAP service and specifies the LDAP server query mode	page 1090
ldap-server	Configures the LDAP server settings	page 1091
ldap-timeout	Configures the LDAP query timeout interval	page 1092
no	Negates a command or reverts settings to their default	page 1093
user-role	Creates a role and associates it to the newly created role policy	page 1095
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

default-role

role-policy

Assigns a default role to a wireless client that fails to match any of the user-defined roles

When a wireless client accesses a network, the client's details, retrieved from the LDAP server, are matched against all user-defined roles within the role policy. If the client fails to match any of these user-defined role filters, the client is assigned the default role. The action taken (permit or deny access) is determined by the IP and/or MAC ACL associated with the default role.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
default-role use [ip-access-list|mac-access-list]
```

```
default-role use [ip-access-list|mac-access-list] [in|out]
<IP/MAC-ACCESS-LIST-NAME>
          precedence <1-100>
```

Parameters

```
default-role use [ip-access-list|mac-access-list] [in|out]
<IP/MAC-ACCESS-LIST-NAME>
precedence <1-100>
```

default-role use	Enables default role configuration. This role is applied to a wireless client not matching any of the user-define roles. • Use – Associates an IP or a MAC access list with the default role
[ip-access-list| mac-access-list] [in|out] <IP/MAC-ACCESS-LIST-NAME>	Associates an IP access list or a MAC access list with this default role • in – Applies the rule (IP or MAC) to incoming packets • out – Applies the rule (IP or MAC) to outgoing packets IP and MAC *access control lists* (ACLs) act as firewalls by blocking and/or permitting data traffic in both directions (inbound and outbound) within a managed network. IP ACLs use IP addresses for matching operations. Whereas, MAC ACLs use MAC addresses for matching operations, In case of a match (i.e. if a packet is received from or is destined for a specified IP or MAC address), an action is taken. This action is a typical allow, deny or mark designation to controller packet traffic. For more information on ACLs, see *ACCESS-LIST*. • <IP/MAC-ACCESS-LIST-NAME> – Specify the IP/MAC access list name. The IP and MAC ACL determine the action applied to a client assigned the default role.
precedence <1-100>	The following keyword is common to the IP and MAC access list parameters: • precedence – Assigns a precedence value to the IP or MAC access list rule identified in the previous step. • <1-100> – Specify a precedence from 1 - 100. Rules with lower precedence are given priority.

Example

```
rfs7000-37FABE(config-role-policy-test)#default-role use ip-access-list in
test precedence 1

rfs7000-37FABE(config-role-policy-test)#show context
role-policy test
 default-role use ip-access-list in test precedence 1
rfs7000-37FABE(config-role-policy-test)#
```

Related Commands:

no	Removes or resets the default role configuration

ldap-deadperiod

role-policy

Configures the *Lightweight Directory Access Protocol* (LDAP) deadperiod interval

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
ldap-deadperiod <60-300>
```

Parameters

```
ldap-deadperiod <60-300>
```

ldap-deadperiod <60-300>	Configures a LDAP dead period. When enabled, LDAP service allows the AP or controller to bind with the LDAP server and retrieve user details to match with user-defined role filters. The LDAP deadperiod is the interval between two consecutive attempts to bind with the LDAP server. To enable LDAP service, use the *ldap-query* command. • <60-300> – Specify the interval from 60 - 600 seconds. The default is 120 seconds.

Example

```
rfs7000-37FABE(config-role-policy-test)#ldap-deadperiod 100

rfs7000-37FABE(config-role-policy-test)#show context
role-policy test
 default-role use ip-access-list in test precedence 1
 ldap-deadperiod 100
rfs7000-37FABE(config-role-policy-test)#
```

Related Commands:

no	Removes or resets the LDAP deadperiod interval

ldap-query

role-policy

Enables LDAP service and specifies the LDAP server query mode

Configuring the LDAP server query mode automatically enables LDAP service on this role policy. By default LDAP service is disabled.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
ldap-query [self|through-controller]
```

Parameters

```
ldap-query [self|through-controller]
```

self	Configures LDAP query mode as self. The AP directly queries the LDAP server for user information. Select 'self' to use local LDAP server resources configured using the *ldap-server* command.
through-controller	Configures LDAP query mode as through-controller. The AP queries the LDAP server, for user information, through the controller. Use this option when the AP is layer 2 adopted to the controller.

Example

```
rfs7000-37FABE(config-role-policy-test)#ldap-query self
rfs7000-37FABE(config-role-policy-test)#

rfs7000-37FABE(config-role-policy-test)#show context
role-policy test
 default-role use ip-access-list in test precedence 1
 ldap-query self
 ldap-deadperiod 100
rfs7000-37FABE(config-role-policy-test)#
```

Related Commands:

no	Disables LDAP service on this role policy

ldap-server

role-policy

Associates a specified LDAP server with this role policy. Use this command to configure the credentials needed to bind with the LDAP server.

When enabled, LDAP service allows the AP or controller to bind with the LDAP server and retrieve user details. This information is matched with the user-defined roles within the role policy. If a match is made, the user is assigned the role and allowed or denied access to the controller managed network.

You can associate two LDAP servers with a role policy, allowing failover in case the primary server is unreachable.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
ldap-server <1-2> host [<IP>|<FQDN>] bind-dn <BIND-DN> base-dn <BASE-DN>
          bind-password <PASSWORD> {port <1-65535>} {(server-type
[active-directory|
          openldap])}
```

Parameters

```
ldap-server <1-2> host [<IP>|<HOSTNAME>] bind-dn <BIND-DN> base-dn <BASE-DN>
bind-password <PASSWORD> {port <1-65535>} {(server-type
[active-directory|openldap])}
```

ldap-server <1-2>	Specify the LDAP server ID from 1 - 2. The primary LDAP server (ID 1) is used to bind and query. The secondary LDAP server (ID 2) is for failover.
host [<IP>|<FQDN>]	Specify the LDAP server's IP address or *Fully Qualified Domain Name* (FQDN).
bind-dn <BIND-DN>	Specify the bind distinguished name (used for binding with the server).
base-dn <BASE-DN>	Specify the base distinguished name (used for searching). This should not exceed 127 characters.
bind-password <PASSWORD>	Specify the LDAP server password associated with the bind DN.
port <1-65535>	Optional. Specify the LDAP server port from 1 - 65535. (default is 389).

server-type [active-directory| openldap]	The following keywords are common to the 'port' parameter:
	• server-type – Optional. Specifies the LDAP server type
	  • active-directory – Enables support for active directory attribute search. This is the default setting.
	  • openldap – Enables support for openLDAP attribute search

Usage Guidelines:

Use the ldap-query command to enable LDAP service on a role policy.

Use the show > role > ldap-stats command to view LDAP server status and state.

Example

```
rfs7000-37FABE(config-role-policy-test)#ldap-server 1 host 192.168.13.7
bind-dn
"CN=Administrator,CN=Users,DC=TechPub,DC=com" base-dn
"CN=Administrator,CN=Users,
DC=TechPub,DC=com" bind-password 0 superuser port 2
rfs7000-37FABE(config-role-policy-test)#

rfs7000-37FABE(config-role-policy-test)#show context
role-policy test
 default-role use ip-access-list in test precedence 1
 ldap-query self
 ldap-deadperiod 100
 ldap-server 1 host 192.168.13.7 bind-dn
CN=Administrator,CN=Users,DC=TechPub,DC=com base-dn
CN=Administrator,CN=Users,DC=com bind-password 0 superuser port 2
rfs7000-37FABE(config-role-policy-test)#
```

Related Commands:

no	Removes or resets the LDAP server settings

ldap-timeout

role-policy

Configures the LDAP timeout interval. This is the interval after which a LDAP query is timed out.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
ldap-timeout <1-5>
```

Parameters

```
ldap-timeout <1-5>
```

ldap-timeout <1-5>	Configures the LDAP query timeout interval from 1 - 5 seconds (default is 2 seconds) When enabled, LDAP service allows the AP or controller to bind with the LDAP server and query it for user details. The LDAP query timeout is the interval between a request to and the response from the LDAP server. Once this interval is exceeded, the LDAP bind and query is timed out.

Example

```
rfs7000-37FABE(config-role-policy-test)#ldap-timeout 1

rfs7000-37FABE(config-role-policy-test)#show context
role-policy test default-role use ip-access-list in test precedence 1
 ldap-query self
 ldap-timeout 1
 ldap-deadperiod 100
 ldap-server 1 host 192.168.13.7 bind-dn
CN=Adminstrator,CN=Users,DC=TechPub,DC=com base-dn
CN=Administrator,CN=Users,DC=com bind-password 0 superuser port 2
rfs7000-37FABE(config-role-policy-test)#
```

Related Commands:

no	Removes or resets the LDAP query timeout to default (2 seconds)

no

role-policy

Negates a command or resets settings to their default. When used in the config role policy mode, the *no* command removes or resets the role policy settings.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no [default-role|ldap-deadperiod|ldap-query|ldap-server
<1-2>|ldap-timeout|user-role]

no [ldap-deadperiod|ldap-query|ldap-server <1-2>|ldap-timeout]
```

```
no default-role use [ip-access-list|mac-access-list]
no default-role use [ip-access-list|mac-access-list] [in|out]
<IP/MAC-ACCESS-LIST-NAME>
          precedence <1-100>

no user-role <ROLE-NAME>
```

Parameters

```
no [ldap-deadperiod|ldap-query|ldap-server <1-2>|ldap-timeout]
```

no ldap-deadperiod	Resets the LDAP dead period interval to default (120 seconds)
no ldap-query	Disables LDAP service on a role policy
no ldap-server <1-2>	Removes the selected LDAP server settings. Specify the LDAP server ID.
no ldap-timeout	Resets the LDAP timeout to default (2 seconds)

```
no default-role use [ip-access-list|mac-access-list] [in|out]
<IP/MAC-ACCESS-LIST-NAME> precedence <1-100>
```

no default-role use	Removes or resets default role configuration • Use – Disables the use of an IP or MAC access list
[ip-access-list| mac-access-list] [in|out]	Disables use of an IP access list or a MAC access list • in – Removes the rule applied to incoming packets • out – Removes the rule applied to outgoing packets
<IP/MAC-ACCESS-LIST-NAME>	Specifies the IP or MAC access list to remove • <IP/MAC-ACCESS-LIST-NAME> – Specify the IP or MAC access list name.
precedence <1-100>	The following keywords are common to the IP and MAC access list parameters: • precedence – Specifies the ACL's precedence • <1-100> – Specify the precedence from 1 - 100. The system removes the access list rule identified by the specified precedence.

```
no user-role <ROLE-NAME>
```

no user-role <ROLE-NAME>	Deletes a user-defined role • <ROLE-NAME> – Specify user-defined role name.

Example

```
The following example shows the role policy 'test' setting before the 'no'
commands are executed:

rfs7000-37FABE(config-role-policy-test)#show context
role-policy test
 default-role use ip-access-list in test precedence 1
 ldap-query self
 ldap-timeout 1
 ldap-deadperiod 100
 ldap-server 1 host 192.168.13.7 bind-dn
CN=Adminstrator,CN=Users,DC=TechPub,DC=com base-dn
CN=Administrator,CN=Users,DC=com bind-password 0 superuser port 2

rfs7000-37FABE(config-role-policy-test)#

rfs7000-37FABE(config-role-policy-test)#no ldap-deadperiod
rfs7000-37FABE(config-role-policy-test)#no ldap-timeout
rfs7000-37FABE(config-role-policy-test)#no ldap-server 1
```

```
The following example shows the role policy 'test' setting after the 'no'
commands are executed:

rfs7000-37FABE(config-role-policy-test)#show context
role-policy test
 default-role use ip-access-list in test precedence 1
 ldap-query self
rfs7000-37FABE(config-role-policy-test)#
```

Related Commands:

default-role	Assigns a default role to a wireless client
ldap-deadperiod	Configures the LDAP deadperiod interval
ldap-query	Enables LDAP service on a role policy
ldap-server	Configures the LDAP server settings
ldap-timeout	Configures the LDAP server query timeout
user-role commands	Creates a role and associates it to the newly created role policy

user-role

role-policy

This command creates a user-defined role. Each user-defined role has a set of Active Directory attributes. Each attribute is matched against the information returned by the LDAP server, until a complete match of role is found.

The following table summarizes user role configuration commands.

user-role	Creates a new user role and enters its configuration mode	page 1095
user-role commands	Summarizes user role configuration mode commands	page 1097

user-role

user-role

Creates a user-defined role. Each role consists of a set of filters and action. The filters are match criteria used to filter wireless clients. And the action defines the action taken when a client matches the specified filters.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
user-role <ROLE-NAME> precedence <1-10000>
```

Parameters

`user-role <ROLE-NAME> precedence <1-10000>`

user-role <ROLE-NAME>	Configures the user role name • <ROLE-NAME> Specify a name for this user role.
precedence <1-10000>	Sets the precedence for this role Lower the precedence, higher is the role priority. Precedence determines the order in which a role is applied. If a wireless client matches multiple roles, the role with the lower precedence is applied before those with higher precedence. While there is no default precedence for a role, two or more roles can share the same precedence.

Example

```
rfs7000-37FABE(config-role-policy-test)#user-role testing precedence 10
rfs7000-37FABE(config-role-policy-test)#show context
role-policy test
 user-role testing precedence 10
 default-role use ip-access-list in test precedence 1
rfs7000-37FABE(config-role-policy-test)#

rfs7000-37FABE(config-role-policy-test-user-role-testing)#?
Role Mode commands:
  br-location          AP Location configuration
  assign               Assign parameters to the role
  authentication-type  Type of Authentication
  captive-portal       Captive-portal based Role Filter
  city                 City configuration
  client-identity      Client identity
  company              Company configuration
  country              Country configuration
  department           Department configuration
  emailid              Emailid configuration
  employee-type        Employee-type configuration
  employeeid           Employeeid configuration
  encryption-type      Type of encryption
  group                Group configuration
  memberOf             MemberOf configuration
  mu-mac               MU MAC address configuration
  no                   Negate a command or set its defaults
  ssid                 SSID configuration
  state                State configuration
  title                Title configuration
  use                  Set setting to use
  user-defined         User-defined configuration
  clrscr               Clears the display screen
  commit               Commit all changes made in this session
  do                   Run commands from Exec mode
  end                  End current mode and change to EXEC mode
  exit                 End current mode and down to previous mode
  help                 Description of the interactive help system
  revert               Revert changes
  service              Service Commands
  show                 Show running system information
  write                Write running configuration to memory or terminal
rfs7000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands:

no	Removes an existing user role

user-role commands

user-role

The following table summarizes user role configuration mode commands.

Commands	Description	Reference
br-location	Configures an AP deployment location based filter	page 1098
assign	Configures upstream/downstream rate limits and VLAN ID assigned to clients matching the filters defined in the user-defined role	page 1099
authentication-type	Configures an authentication type based filter	page 1101
captive-portal	Configures a captive portal based filter	page 1102
city	Configures a city name based filter	page 1103
client-identity	Associates a client-identity (device fingerprinting) based filter	page 1104
company	Configures a company name based filter	page 1105
country	Configures a country name based filter	page 1106
department	Configures a department name based filter	page 1107
emailid	Configures a e-mail ID based filter	page 1108
employee-type	Configures a employee type ID based filter	page 1109
employeeid	Configures a employee ID based filter	page 1110
encryption-type	Configures an encryption type filter	page 1111
group	Configures a RADIUS group based filter	page 1112
memberOf	Assigns an *Active Directory* (AD) group to this user-defined role	page 1114
mu-mac	Configures MAC address and mask based filter	page 1114
no	Removes or resets the filters configured on this user-defined role	page 1115
ssid	Configures a SSID based filter	page 1118
state	Configures a user role state to match	page 1119
title	Configures a 'title' string to match	page 1120
use	Associates a IP and/or MAC ACL with this role. These ACLs specify the action taken when a client matches this user-defined role.	page 1121
user-defined	Defines a filter based on an attribute defined in the Active Directory or the OpenLDAP server	page 1123
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394

Commands	Description	Reference
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

br-location

user-role commands

Configures an AP's deployment location based filter for this user-defined role

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
br-location [any|contains|exact|not-contains]

br-location any

br-location [contains|exact|not-contains] <WORD>
```

Parameters

```
br-location any
```

br-location any	Specifies the AP location to match (in a RF Domain) or the AP's resident configuration • any – Defines an AP's location as any

```
br-location [contains|exact|not-contains] <WORD>
```

br-location	Specifies the AP location to match (in a RF Domain) or the AP's resident configuration. Select one of the following filter options: contains, exact, or not-contains.
contains <WORD>	Applies role if the associating AP's location contains the location string specified in the role. • <WORD> – Specify the location string to match.
exact <WORD>	Applies role if the associating AP's location exactly matches the string specified in the role. • <WORD> – Specify the exact location string to match.
not-contains <WORD>	Applies role if the associating AP's location does not contain the location string specified in the role. • <WORD> – Specify the location string not to match.

Example

```
rfs7000-37FABE(config-role-policy-test-user-role-testing)#br-location
contains office

rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
  br-location contains office
rfs7000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands:

no	Removes an AP's deployment location string from this user-defined role

assign

user-role commands

Configures upstream/downstream rate limits and VLAN ID. Clients matching this user-defined role filters are associated with the specified VLAN, and assigned the specified data rates.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
assign [rate-limit|VLAN]

assign rate-limit [from-client|to-client] <1-65536>
assign vlan <1-4094>
```

Parameters

```
assign rate-limit [from-client|to-client] <1-65536>
```

assign rate-limit [from-client|to-client] <1-65536>	Assigns an upstream and downstream traffic rate limit • from-client – Assigns a rate limit, in Kbps, for the upstream (from client) traffic • to-client – Assigns a rate limit, in Kbps, for the downstream (to client) traffic • <1-65536> – Specify upstream and/or downstream rate limits from 1 - 65536 Kbps. Wireless clients matching this user-defined role are assigned the configured rate limits.

```
assign vlan <1-4094>
```

assign vlan <1-4094>	Assigns a VLAN (identified by VLAN's ID). Clients matching this user-defined role are associated with the specified VLAN. The VLAN ID represents the shared SSID each user employs to interoperate within the network (once authenticated by the local RADIUS server). This feature is disabled by default. • <1-4094> – Specify the VLAN ID from 1 - 4094. A wireless client that fails to match any user-defined role is assigned to the default role (configured as a role policy setting) and is mapped to the default VLAN under the WLAN.

Usage Guidelines:

ACLs can only be used with tunnel or isolated-tunnel modes. They do not work with the local and automatic modes.

In case of bridge VLAN, the default bridging mode is 'auto'. Change the bridging mode to 'tunnel'. This extends the controller's existing VLAN onto the AP and ensures that wireless clients are served IP addresses.

The VLAN configured under the user-defined role need not exist under the WLAN. But, when using tunneled VLAN bridges, configure an additional bridge VLAN. If the VLAN bridging mode is 'local', no additional VLAN configuration is required.

Example

```
rfs4000-229D58(config-role-policy-test-user-role-test)#assign rate-limit
to-client 200
rfs4000-229D58(config-role-policy-test-user-role-test)#

rfs4000-229D58(config-role-policy-test-user-role-test)#commit
rfs4000-229D58(config-role-policy-test-user-role-test)#

rfs4000-229D58(config-role-policy-test-user-role-test)#show context
 user-role test precedence 1
  assign vlan 1
  assign rate-limit to-client 200
rfs4000-229D58(config-role-policy-test-user-role-test)#

The following examples define a role used to forward the IP traffic from all
engineers in Brocade onto vlan 2.

Create a new role policy with name ‘motorola-policy’.

<DEVICE>(config)#role-policy motorola-policy

Specify the LDAP server used for this role policy.

<DEVICE>(config-role-policy-motorola-policy)#ldap-query self

<DEVICE>(config-role-policy-motorola-policy)#ldap-server 1 host 192.160.1.1
bind-dn CN=Administrator,CN=Users,DC=motorolaMotorola,DC=com base-dn
CN=Administrator,CN=Users,DC=com bind-password 0 Motorola port 389

<DEVICE>(config-role-policy-motorola-policy)#ldap-timeout 2

Create a user defined role.

<DEVICE>(config-role-policy-motorola-policy)#user-role SCEngineer precedence
100

Define the role by adding appropriate values and match operators.

<DEVICE>(config-role-policy-motorola-policy-user-role-SCEngineer)#city exact
santa-clara
<DEVICE>(config-role-policy-motorola-policy-user-role-SCEngineer)#company
exact motorola
<DEVICE>(config-role-policy-motorola-policy-user-role-SCEngineer)#country
exact usa
<DEVICE>(config-role-policy-motorola-policy-user-role-SCEngineer)#title
contains engineer
<DEVICE>(config-role-policy-motorola-policy-user-role-SCEngineer)#assign
vlan-id 2

Apply role policy to an access point.

br7131-99BFA8(config-device-br7131)# use role-policy motorola-policy
```

Related Commands:

no	Removes the upstream and/or downstream rate limits applied to this user-defined role. Also removes the VLAN ID.

authentication-type

user-role commands

Configures the authentication type based filter for this user-defined role

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
authentication-type [any|eq|neq]
authentication-type any
authentication-type [eq|neq] [eap|kerberos|mac-auth|none]
          {(eap|kerberos|mac-auth|none)}
```

Parameters

```
authentication-type any
```

any	The authentication type is any (eq or neq). This is the default setting.

```
authentication-type [eq|neq] [eap|kerberos|mac-auth|none]
{(eap|kerberos|mac-auth|
none)}
```

eq [eap|kerberos|mac-auth|none]	The role is applied only when the authentication type matches (equals) one or more than one of the following types: • eap – Extensible authentication protocol • kerberos – Kerberos authentication • mac-auth – MAC authentication protocol • none – no authentication used These parameters are recursive, and you can configure more than one unique authentication type for this user-defined role.
neq [eap|kerberos|mac-auth|none]	The role is applied only when the authentication type does not match (not equals) any of the following types: • eap – Extensible authentication protocol • kerberos – Kerberos authentication • mac-auth – MAC authentication protocol • none – no authentication used These parameters are recursive, and you can configure more than one unique 'not equal to' authentication type for this user-defined role.

Example

```
rfs7000-37FABE(config-role-policy-test-user-role-testing)#authentication-type
eq kerberos

rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
  authentication-type eq kerberos
  br-location contains office
rfs7000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands:

no	Removes the authentication type filter configured for this user-defined role

captive-portal

user-role commands

Configures a captive portal based filter for this user-defined role. A captive portal is a guest access policy that provides temporary and restrictive access to the wireless network. When applied to a WLAN, a captive portal policy ensures secure guest access.

This command defines user-defined role filters based on a wireless client's state of authentication.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
captive-portal authentication-state [any|post-login|pre-login]
```

Parameters

```
captive-portal authentication-state [any|post-login|pre-login]
```

authentication-state	Defines the authentication state of a client connecting to a captive portal
any	Specifies any authentication state (authenticated and pending authentication). This is the default setting. This option makes no distinction on whether authentication is conducted before or after the wireless client has logged in.
post-login	Specifies authentication is completed successfully This option requires the wireless client to share authentication credentials after logging into the managed network.
pre-login	Specifies authentication is pending This option enables captive portal client authentication before the client is logged into the controller

Example

```
rfs7000-37FABE(config-role-policy-test-user-role-testing)#captive-portal
authentication-state pre-login

rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
  authentication-type eq kerberos
  br-location contains office
  captive-portal authentication-state pre-login
rfs7000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands:

no	Removes the captive portal based role filter settings

city

user-role commands

Configures a wireless client filter based on the city name

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
city [any|contains|exact|not-contains]
city [any|exact <WORD>|contains <WORD>|not-contains <WORD>]
```

Parameters

```
city [any|exact <WORD>|contains <WORD>|not-contains <WORD>]
```

city	Specifies a wireless client filter based on how the 'city' name, returned by the RADIUS server, matches the provided expression. Select one of the following options: any, contains, exact, or not-contain.
any	No specific city associated with this user-defined role. This role can be applied to any wireless client from any city.
contains <WORD>	The role is applied only when the city name, returned by the RADIUS server, contains the string specified in the role. • <WORD> – Specify the string to match (this is case sensitive, and is compared against the city name returned by the RADIUS server). It should contain the provided expression.
exact	The role is applied only when the city name, returned by the RADIUS server, exactly matches the string specified in the role. • <WORD> – Specify the exact string to match (this is case sensitive, and is compared against the city name returned by the RADIUS server). It should be an exact match.
not-contains <WORD>	The role is applied only when the city name, returned by the RADIUS server, does not contain the string specified in the role. • <WORD> – Specify the string not to match (this is case sensitive, and is compared against the city name returned by the RADIUS server). It should not contain the provided expression.

Example

```
rfs7000-37FABE(config-role-policy-test-user-role-testing)#city exact SanJose

rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
  authentication-type eq kerberos
  br-location contains office
  captive-portal authentication-state pre-login
  city exact SanJose
rfs7000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands:

no	Removes the city name configured with this user-defined role

client-identity

user-role commands

Associates a client-identity (device fingerprinting) based filter. The role is assigned to a wireless client matching any of the defined client identities.

For more information on configuring client identity fingerprints, see *client-identity*.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
client-identity <CLIENT-IDENTITY-NAME> {<CLIENT-IDENTITY-NAME>}
```

Parameters

```
client-identity <CLIENT-IDENTITY-NAME> {<CLIENT-IDENTITY-NAME>}
```

client-identity <CLIENT-IDENTITY-NAME>	Specifies the client-identity fingerprint to match (should be existing and configured) • <CLIENT-IDENTITY-NAME> – Specify the client identity signature name. Multiple client identities can be configured with a role policy.

Usage Guidelines:

When associating a single or multiple client identities with a role policy, ensure that a client identity group, containing all the client identities used by the role policy, is attached to the device or profile using the role policy. In other words, group all the client identities (used in this role policy) in a client identity group, and associate this group to the profile or device using this role policy.

For more information on configuring client identities and client identity groups, see *client-identity*, and *client-identity-group*.

For more information on associating a client identity group and a role policy to a profile or a device, see *use*.

Example

```
rfs4000-229D58(config-role-policy-test-user-role-test)#client-identity
TestClientIdentity
rfs4000-229D58(config-role-policy-test-user-role-test)#commit

rfs4000-229D58(config-role-policy-test-user-role-test)#client-identity
ClientIdentityWindows
rfs4000-229D58(config-role-policy-test-user-role-test)#

rfs4000-229D58(config-role-policy-test-user-role-test)#show context
 user-role test precedence 1
  client-identity TestClientIdentity
  client-identity ClientIdentityWindows
rfs4000-229D58(config-role-policy-test-user-role-test)#
```

Related Commands:

no	Removes the client identities associated with this role policy

company

user-role commands

Configures a wireless client filter based on the company name

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
company [any|contains|exact|not-contains]
company [any|exact <WORD>|contains <WORD>|not-contains <WORD>]
```

Parameters

```
company [any|exact <WORD>|contains <WORD>|not-contains <WORD>]
```

company	Specifies a wireless client filter based on how the 'company' name, returned by the RADIUS server, matches the provided expression. Select one of the following options: any, contains, exact, or not-contains
any	No specific company associated with this user-defined role. This role is applied to any wireless client from any company (no strings to match). This is the default setting.
contains <WORD>	The role is applied only when the company name, returned by the RADIUS server, contains the string specified in the role. • <WORD> – Specify the string to match (this is case sensitive, and is compared against the company name returned by the RADIUS server). It should contain the provided expression.
exact	The role is applied only when the company name, returned by the RADIUS server, exactly matches the string specified in the role. • <WORD> – Specify the exact string to match (this is case sensitive, and is compared against the company name returned by the RADIUS server). It should be an exact match.
not-contains <WORD>	The role is applied only when the company name, returned by the RADIUS server, does not contain the string specified in the role. • <WORD> – Specify the string not to match (this is case sensitive, and is compared against the company name returned by the RADIUS server). It should not contain the provided expression.

Example

```
rfs7000-37FABE(config-role-policy-test-user-role-testing)#company exact
MotorolaSolutions

rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
  authentication-type eq kerberos
  br-location contains office
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact MotorolaSolutions
```

```
rfs7000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands:

no	Removes the company name configured with this user-defined role

country

user-role commands

Configures a wireless client filter based on the country name

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
country [any|contains|exact|not-contains]
country [any|exact <WORD>|contains <WORD>|not-contains <WORD>]
```

Parameters

```
country [any|exact <WORD>|contains <WORD>|not-contains <WORD>]
```

country	Specifies a wireless client filter based on how the 'country' name, returned by the RADIUS server, matches the provided expression. Select one of the following options: any, contains, exact, or not-contains
any	No specific country associated with this user-defined role. This role is applied to any wireless client from any country (no strings to match). This is the default setting.
contains <WORD>	The role is applied only when the country name, returned by the RADIUS server, contains the string specified in the role. • <WORD> – Specify the string to match (this is case sensitive, and is compared against the country name returned by the RADIUS server). It should contain the provided expression.
exact	The role is applied only when the country name, returned by the RADIUS server, exactly matches the string specified in the role. • <WORD> – Specify the exact string to match (this is case sensitive, and is compared against the country name returned by the RADIUS server). It should be an exact match.
not-contains <WORD>	The role is applied only when the country name, returned by the RADIUS server, does not contain the string specified in the role. • <WORD> – Specify the string not to match (this is case sensitive, and is compared against the country name returned by the RADIUS server). It should not contain the provided expression.

Example

```
rfs7000-37FABE(config-role-policy-test-user-role-testing)#country exact
America

rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
  authentication-type eq kerberos
  br-location contains office
  captive-portal authentication-state pre-login
```

```
  city exact SanJose
  company exact MotorolaSolutions
  country exact America
rfs7000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands:

no	Removes the country name configured with this user-defined role

department

user-role commands

Configures a wireless client filter based on the department name

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
department [any|contains|exact|not-contains]
department [any|exact <WORD>|contains <WORD>|not-contains <WORD>]
```

Parameters

```
department [any|exact <WORD>|contains <WORD>|not-contains <WORD>]
```

department	Specifies a wireless client filter based on how the 'department' name, returned by the RADIUS server, matches the provided expression. Select one of the following options: any, contains, exact, or not-contains
any	No specific department associated with this user-defined role. This role can be applied to any wireless client from any department (no strings to match). This is the default setting.
contains <WORD>	The role is applied only when the department name, returned by the RADIUS server, contains the string specified in the role. • <WORD> – Specify the string to match (this is case sensitive, and is compared against the department name returned by the RADIUS server). It should contain the provided expression.
exact	The role is applied only when the department name, returned by the RADIUS server, exactly matches the string specified in the role. • <WORD> – Specify the exact string to match (this is case sensitive, and is compared against the department name returned by the RADIUS server). It should be an exact match.
not-contains <WORD>	The role is applied only when the department name, returned by the RADIUS server, does not contain the string specified in the role. • <WORD> – Specify the string not to match (this is case sensitive, and is compared against the department name returned by the RADIUS server). It should not contain the provided expression.

Example

```
rfs7000-37FABE(config-role-policy-test-user-role-testing)#department exact
TnV

rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
```

```
    authentication-type eq kerberos
    br-location contains office
    captive-portal authentication-state pre-login
    city exact SanJose
    company exact MotorolaSolutions
    country exact America
    department exact TnV
rfs7000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands:

no	Removes the department name configured with this user-defined role

emailid

user-role commands

Configures a wireless client filter based on the e-mail ID

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
emailid [any|contains|exact|not-contains]
emailid [any|exact <WORD>|contains <WORD>|not-contains <WORD>]
```

Parameters

```
emailid [any|exact <WORD>|contains <WORD>|not-contains <WORD>]
```

emailid	Specifies a wireless client filter based on how the 'e-mail ID', returned by the RADIUS server, matches the provided expression. Select one of the following options: any, contains, exact, or not-contains
any	No specific e-mail ID associated with this user-defined role. This role can be applied to any wireless client having any e-mail ID (no strings to match). This is the default setting.
contains <WORD>	The role is applied only when the e-mail ID, returned by the RADIUS server, contains the string specified in the role. • <WORD> – Specify the string to match (this is case sensitive, and is compared against the e-mail ID returned by the RADIUS server). It should contain the provided expression.
exact	The role is applied only when the e-mail ID, returned by the RADIUS server, exactly matches the string specified in the role. • <WORD> – Specify the exact string to match (this is case sensitive, and is compared against the e-mail ID returned by the RADIUS server). It should be an exact match.
not-contains <WORD>	The role is applied only when the e-mail ID, returned by the RADIUS server, does not contain the string specified in the role. • <WORD> – Specify the string not to match (this is case sensitive, and is compared against the e-mail ID returned by the RADIUS server). It should not contain the provided expression.

Example

```
rfs7000-37FABE(config-role-policy-test-user-role-testing)#emailid exact
testing@
motorolasolutions.com

rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
  authentication-type eq kerberos
  br-location contains office
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact MotorolaSolutions
  country exact America
  department exact TnV
  emailid exact testing@motorolasolutions.com
rfs7000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands:

no	Removes the e-mail ID configured with this user-defined role

employee-type

user-role commands

Configures a wireless client filter based on the employee type

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
employee-type [any|contains|exact|not-contains]
employee-type [any|exact <WORD>|contains <WORD>|not-contains <WORD>]
```

Parameters

```
employee-type [any|exact <WORD>|contains <WORD>|not-contains <WORD>]
```

employee-type	Specifies a wireless client filter based on how the 'employee type', returned by the RADIUS server, matches the provided expression. Select one of the following options: any, contains, exact, or not-contains.
any	No specific employee type associated with this user-defined role. This role can be applied to any wireless client having any employee type (no strings to match). This is the default setting.
contains <WORD>	The role is applied only when the employee type, returned by the RADIUS server, contains the string specified in the role. • <WORD> – Specify the string to match (this is case sensitive, and is compared against the employee type returned by the RADIUS server). It should contain the provided expression.

exact	The role is applied only when the employee type, returned by the RADIUS server, exactly matches the string specified in the role. • <WORD> – Specify the exact string to match (this is case sensitive, and is compared against the employee type returned by the RADIUS server). It should be an exact match.
not-contains <WORD>	The role is applied only when the employee type, returned by the RADIUS server, does not contain the string specified in the role. • <WORD> – Specify the string not to match (this is case sensitive, and is compared against the employee type returned by the RADIUS server). It should not contain the provided expression.

Example

```
rfs4000-229D58(config-role-policy-test-user-role-test1)#employee-type exact
consultant

rfs4000-229D58(config-role-policy-test-user-role-user1)#show context
 user-role user1 precedence 1
  employee-type exact consultant
rfs4000-229D58(config-role-policy-test-user-role-user1)#
```

Related Commands:

no	Removes the employee type filter configured with this user-defined role

employeeid

user-role commands

Configures a wireless client filter based on the employee ID

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
employeeid [any|contains|exact|not-contains]
employeeid [any|exact <WORD>|contains <WORD>|not-contains <WORD>]
```

Parameters

```
employeeid [any|exact <WORD>|contains <WORD>|not-contains <WORD>]
```

employeeid	Specifies a wireless client filter based on how the 'employee ID', returned by the RADIUS server, matches the provided expression. Select one of the following options: any, contains, exact, or not-contains.
any	No specific employee ID associated with this user-defined role. This role can be applied to any wireless client having any employee ID (no strings to match). This is the default setting.
contains <WORD>	The role is applied only when the employee ID, returned by the RADIUS server, contains the string specified in the role. • <WORD> – Specify the string to match (this is case sensitive, and is compared against the employee ID returned by the RADIUS server). It should contain the provided expression.

exact	The role is applied only when the employee ID, returned by the RADIUS server, exactly matches the string specified in the role. • <WORD> – Specify the exact string to match (this is case sensitive, and is compared against the employee ID returned by the RADIUS server). It should be an exact match.
not-contains <WORD>	The role is applied only when the employee ID, returned by the RADIUS server, does not contain the string specified in the role. • <WORD> – Specify the string not to match (this is case sensitive, and is compared against the employee ID returned by the RADIUS server). It should not contain the provided expression.

Example

```
rfs7000-37FABE(config-role-policy-test-user-role-testing)#employeeid contains
TnVMoto

rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
  authentication-type eq kerberos
  br-location contains office
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact MotorolaSolutions
  country exact America
  department exact TnV
  emailid exact testing@motorolasolutions.com
  employeeid contains TnVMoto
rfs7000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands:

no	Removes the employee ID configured with this user-defined role

encryption-type

user-role commands

Selects the encryption type for this user-defined role. Encryption ensures privacy between access points and wireless clients. There are various modes of encrypting communication on a WLAN, such as *Counter-model CBC-MAC Protocol* (CCMP), *Wired Equivalent Privacy* (WEP), keyguard, *Temporal Key Integrity Protocol* (TKIP) etc.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
encryption-type [any|eq|neq]

encryption-type any

encryption-type [eq|neq] [ccmp|keyguard|none|tkip|wep128|wep64]
          {(ccmp|keyguard|none|tkip|tkip-ccmp|wep128|wep64)}
```

Parameters

`encryption-type any`

any	The encryption type can be any one of the listed options (ccmp|keyguard|tkip|wep128|wep64). This is the default setting.

`encryption-type [eq|neq] [ccmp|keyguard|none|tkip|wep128|wep64]`
`{(ccmp|keyguard|none|tkip|tkip-ccmp|wep128|wep64)}`

eq [ccmp|keyguard|none|tkip|wep128|wep64]	The role is applied only if the encryption type equals to one of the following options: • ccmp: Encryption mode is CCMP • keyguard: Encryption mode is keyguard. Keyguard encryption shields the master encryption keys from being discovered • none: No encryption mode specified • tkip: Encryption mode is TKIP • wep128: Encryption mode is WEP128 • wep64: Encryption mode is WEP64 These parameters are recursive, and you can configure more than one encryption type for this user-defined role.
neq [ccmp|keyguard|none|tkip|wep128|wep64]	The role is applied only if encryption type is not equal to any of the following options: • ccmp: Encryption mode is not equal to CCMP • keyguard: Encryption mode is not equal to keyguard • none: Encryption mode is not equal to none • tkip: Encryption mode is not equal to TKIP • wep128: Encryption mode is not equal to WEP128 • wep64: Encryption mode is not equal to WEP64 These parameters are recursive, and you can configure more than one 'not equal to' encryption type for this user-defined role.

Example

```
rfs7000-37FABE(config-role-policy-test-user-role-testing)#encryption-type eq
wep128

rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
  authentication-type eq kerberos
  encryption-type eq wep128
  br-location contains office
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact MotorolaSolutions
  country exact America
  department exact TnV
  emailid exact testing@motorolasolutions.com
  employeeid contains TnVMoto
rfs7000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands:

no	Removes the encryption type configured for this user-defined role

group

user-role commands

Configures a wireless client filter based on the RADIUS group name

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
group [any|contains|exact|not-contains]
group [any|contains <WORD>|exact <WORD>|not-contains <WORD>]
```

Parameters

```
group [any|contains <WORD>|exact <WORD>|not-contains <WORD>]
```

group	Specifies a wireless client filter based on how the RADIUS group name matches the provided expression. Select one of the following options: any, contains, exact, or not-contains
any	This user-defined role can fit into any group (no strings to match). This is the default setting.
contains <WORD>	The role is applied only when the RADIUS group name contains the string specified in the role. • <WORD> – Specify the string to match (this is case sensitive, and is compared against the group name returned by the RADIUS server). It should contain the provided expression.
exact <WORD>	The role is applied only when the RADIUS group name exactly matches the string specified in the role. • <WORD> – Specify the exact string to match (this is case sensitive, and is compared against the group name returned by the RADIUS server). It should be an exact match.
not-contains <WORD>	The role is applied only when the RADIUS group name does not contain the string specified in the role. • <WORD> – Specify the string not to match (this is case sensitive, and is compared against the group name returned by the RADIUS server). It should not contain the provided expression.

Example

```
rfs7000-37FABE(config-role-policy-test-user-role-testing)#group contains
testgroup

rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
  authentication-type eq kerberos
  encryption-type eq wep128
  br-location contains office
  group contains testgroup
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact MotorolaSolutions
  country exact America
  department exact TnV
  emailid exact testing@motorolasolutions.com
  employeeid contains TnVMoto
rfs7000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands:

no	Removes the group configured for this user-defined role

memberOf

user-role commands

Applies an *Active Directory* (AD) group filter to this user-defined role. A wireless client can be a member of more than one group within the AD database. This command applies a AD group based firewall, which applies a role to a wireless client only if it belongs to the specified AD group.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
memberOf <AD-GROUP-NAME>
```

Parameters

```
memberOf <AD-GROUP-NAME>
```

memberOf <AD-GROUP-NAME>	Applies this user-defined role to a client only if the client belongs to the specified AD group • <AD-GROUP-NAME> – Specify the AD group name.

Example

```
rfs4000-229D58(config-role-policy-test-user-role-test)#memberOf ADTestgroup
rfs4000-229D58(config-role-policy-test-user-role-test)#

rfs4000-229D58(config-role-policy-test-user-role-test)#show context
 user-role test precedence 1
  assign vlan 1
  assign rate-limit to-client 200
  memberOf ADTestgroup
rfs4000-229D58(config-role-policy-test-user-role-test)#
```

Related Commands:

no	Removes the AD group assigned to this user-defined role

mu-mac

user-role commands

Configures a MAC address and mask based filter for this role policy

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
mu-mac [<MAC>|any]

mu-mac any

mu-mac <MAC> {mask <MAC>}
```

Parameters

```
mu-mac any
```

any	Applies role to any wireless client (no MAC address to match). This is the default setting.

```
mu-mac <MAC> {mask <MAC>}
```

<MAC>	Applies role to the wireless client having specified MAC address • <MAC> – Sets the MAC address in the AA-BB-CC-DD-EE-FF format
mask <MAC>	Optional. After specifying the client's MAC address, specify the mask in the AA-BB-CC-DD-EE-FF format. The role is applied to the wireless client exactly matching the specified MAC address and MAC mask.

Example

```
rfs7000-37FABE(config-role-policy-test-user-role-testing)#mu-mac
11-22-33-44-55-66

rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
  authentication-type eq kerberos
  encryption-type eq wep128
  br-location contains office
  mu-mac 11-22-33-44-55-66
  group contains testgroup
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact MotorolaSolutions
  country exact America
  department exact TnV
  emailid exact testing@motorolasolutions.com
  employeeid contains TnVMoto
rfs7000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands:

no	Removes the MAC address and mask for this user-defined role

no

user-role commands

Negates a command or resets configured settings to their default. When used in the config role policy user-defined role mode, the no command removes or resets settings, such as AP location, authentication type, encryption type, captive portal etc.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no
[br-location|assign|authentication-type|captive-portal|city|client-identity|

company|country|department|emailid|employee-type|employeeid|encryption-type|
          group|memberOf|mu-mac|ssid|state|title|use|user-defined]

no
[br-location|assign|authentication-type|city|client-identity|company|country|

department|emailid|employee-type|employeeid|encryption-type|group|mu-mac|memb
erOf|
          ssid|state|title|user-defined]

no captive-portal authentication-state

no use [ip-access-list|mac-access-list] [in|out] <IP/MAC-ACCESS-LIST-NAME>
          precedence <1-100>
```

Parameters

```
no
[br-location|assign|authentication-type|city|client-identity|company|country|
department|emailid|employee-type|employeeid|encryption-type|group|mu-mac|memb
erOf|ssid|
state|title|user-defined]
```

no br-location	Removes an AP's deployment location filter
no assign	Removes the upstream and/or downstream rate limits and the VLAN ID associated with this user-defined role
no authentication-type	Removes the authentication type filter
no city	Removes the configured city name filter
no client-identity	Removes the client identity fingerprints based filter
no company	Removes the configured company name filter
no country	Removes the configured country name filter
no department	Removes the configured department name filter
no emailid	Removes the configured e-mail ID filter
no employee-type	Removes the configured employee-type filter
no employeeid	Removes the configured employee ID filter
no encryption-type	Removes the encryption type filter
no group	Removes the RADIUS group name filter
no memberOf	Removes the AD group based filter
no mu-mac	Removes the MAC address and mask filter
no ssid	Removes the SSID filter
no state	Removes the configured state filter

no title	Removes the title filter
no user-defined	Removes the user-defined filter (an attribute defined in the AD or OpenLDAP server)

```
no captive-portal authentication-state
```

no captive-portal	Removes the captive portal based filter
authentication-state	Removes the authentication state filter

```
no use [ip-access-list|mac-access-list] [in|out] <IP/MAC-ACCESS-LIST-NAME>
precedence <1-100>
```

no use	Removes an IP or MAC access list from this user-defined role
[ip-access-list| mac-access-list] [in|out]	Removes the specified IP or MAC access list from a user group • in – Removes the list from being applied to incoming packets • out – Removes the list from being applied to outgoing packets
<IP/MAC-ACCESS-LIST-NAME>	Specifies the IP or MAC access list name
precedence <1-100>	Specifies the access list precedence • <1-100> – Specify the precedence from 1 - 100.

Usage Guidelines:

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
The following example shows the Role Policy ‘test’ User Role ‘testing’
configuration before the ‘no’ commands are executed:

rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
  authentication-type eq kerberos
  encryption-type eq wep128
  br-location contains office
  mu-mac 11-22-33-44-55-66
  group contains testgroup
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact MotorolaSolutions
  country exact America
  department exact TnV
  emailid exact testing@motorolasolutions.com
  employeeid contains TnVMoto
rfs7000-37FABE(config-role-policy-test-user-role-testing)#

rfs7000-37FABE(config-role-policy-test-user-role-testing)#no
authentication-type
rfs7000-37FABE(config-role-policy-test-user-role-testing)#no encryption-type
rfs7000-37FABE(config-role-policy-test-user-role-testing)#no group
rfs7000-37FABE(config-role-policy-test-user-role-testing)#no mu-mac
rfs7000-37FABE(config-role-policy-test-user-role-testing)#no br-location
rfs7000-37FABE(config-role-policy-test-user-role-testing)#no employeeid

The following example shows the Role Policy ‘test’ User Role ‘testing’
configuration after the ‘no’ commands are executed:

rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context
```

```
 user-role testing precedence 10
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact MotorolaSolutions
  country exact America
  department exact TnV
  emailid exact testing@motorolasolutions.com
rfs7000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands:

br-location	Configures an AP deployment location based filter
assign	Configures upstream/downstream rate limits and VLAN ID assigned to clients matching the filters defined in the user-defined role
authentication-type	Configures the authentication type filter
captive-portal	Configures a captive portal based filter
city	Configures a city name based filter
client-identity	Associates a client-identity (device fingerprinting) based filter with this user-defined role
company	Configures a company name based filter
country	Configures a country name based filter
department	Configures a department name based filter
emailid	Configures a e-mail ID based filter
employee-type	Configures a employee type based filter
employeeid	Configures a employee ID based filter
encryption-type	Configures the encryption type filter
group	Configures a RADIUS group based filter
memberOf	Configures an AD group based filter
mu-mac	Configures a MAC address and mask based filter
ssid	Configures a SSID based filter
state	Configures a state name based filter
title	Configures a user title based filter
use	Associates an IP and/or MAC ACL with this user-defined role
user-defined	Configures a user-defined filter (an attribute defined in AD or OpenLDAP server)

ssid

user-role commands

Configures a SSID based filter

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
ssid [any|exact|contains|not-contains]

ssid any

ssid [exact|contains|not-contains] <WORD>
```

Parameters

```
ssid any
```

ssid any	Specifies a wireless client filter based on how the SSID is specified in a WLAN. • any – The role is applied to any SSID location. This is the default setting.

```
ssid [exact|contains|not-contains] <WORD>
```

ssid	Specifies a wireless client filter based on how the SSID is specified in a WLAN. This options are: contains, exact, or not-contains
exact <WORD>	The role is applied only when the SSID, returned by the RADIUS server, exactly matches the string specified in the role. • <WORD> – Specify the SSID string to match. The SSID is case sensitive and is compared against the SSID configured for the WLAN.
contains <WORD>	The role is applied only when the SSID, returned by the RADIUS server, contains the string specified in the role. • <WORD> – Specify the SSID string to match. The SSID is case sensitive and is compared against the SSID configured for the WLAN.
not-contains <WORD>	The role is applied only when the SSID, returned by the RADIUS server, does not contain the string specified in the role. • <WORD> – Specify the SSID string not to match. The SSID is case sensitive and is compared against the SSID configured for the WLAN.

Example

```
rfs7000-37FABE(config-role-policy-test-user-role-testing)#ssid not-contains
DevUser

rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
  ssid not-contains DevUser
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact MotorolaSolutions
  country exact America
  department exact TnV
  emailid exact testing@motorolasolutions.com
rfs7000-37FABE(config-role-policy-test-user-role-testing)#]
```

Related Commands:

no	Removes the SSID configured for a user-defined role

state

user-role commands

Configures a user role state to match with this user-defined role

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
state [any|contains|exact|not-contains]
state [any|contains <WORD>|exact <WORD>|not-contains <WORD>]
```

Parameters

```
state [any|contains <WORD>|exact <WORD>|not-contains <WORD>]
```

state	Specifies a wireless client filter option based on how the RADIUS state matches the provided expression. Select one of the following options: any, contains, exact, or not-contains.
any	This user role can fit any wireless client irrespective of the state (no strings to match).
contains <WORD>	The user role is applied only when the RADIUS state contains the string specified in the role. • <WORD> – Specify the string to match (this is case sensitive, and is compared against the state returned by the RADIUS server). It should contain the provided expression.
exact <WORD>	The role is applied only when the RADIUS state exactly matches the string specified in the role. • <WORD> – Specify the exact string to match (this is case sensitive, and is compared against the state returned by the RADIUS server). It should be an exact match.
not-contains <WORD>	The role is applied only when the RADIUS state does not contain the string specified in the role. • <WORD> – Specify the string not to match (this is case sensitive, and is compared against the state returned by the RADIUS server). It should not contain the provided expression.

Example

```
rfs7000-37FABE(config-role-policy-test-user-role-testing)#state exact active

rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
  ssid not-contains DevUser
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact MotorolaSolutions
  country exact America
  department exact TnV
  emailid exact testing@motorolasolutions.com
  state exact active
rfs7000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands:

no	Removes the ‘state’ filter string associated with a user role

title

user-role commands

Configures a ‘title’ string to match

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
title [any|contains|exact|not-contains]
title [any|contains <WORD>|exact <WORD>|not-contains <WORD>]
```

Parameters

```
title [any|contains <WORD>|exact <WORD>|not-contains <WORD>]
```

title	Specifies a wireless client filter based on how the title string, returned by the RADIUS server, matches the provided expression. Select one of the following options: any, contains, exact, or not-contains.
any	This user role can fit any wireless client irrespective of the title (no strings to match).
contains <WORD>	The user role is applied only when the title string, returned by the RADIUS server, contains the string specified in the role. • <WORD> – Specify the string to match (this is case sensitive, and is compared against the title returned by the RADIUS server). It should contain the provided expression.
exact <WORD>	The role is applied only when the title string, returned by the RADIUS server, exactly matches the string specified in the role. • <WORD> – Specify the exact string to match (this is case sensitive, and is compared against the title returned by the RADIUS server). It should be an exact match.
not-contains <WORD>	The role is applied only when the title string, returned by the RADIUS server, does not contain the string specified in the role. • <WORD> – Specify the string not to match (this is case sensitive, and is compared against the title returned by the RADIUS server). It should not contain the provided expression.

Example

```
rfs7000-37FABE(config-role-policy-test-user-role-testing)#title any
```

Related Commands:

no	Removes the 'title' filter string configured with a user role

use

user-role commands

Configures an access list based firewall with this user role

A firewall is a mechanism enforcing access control, and is considered a first line of defense in protecting proprietary information within the network. The means by which this is accomplished varies, but in principle, firewalls are mechanisms both *blocking* and *permitting* data traffic based on inbound and outbound IP and MAC rules.

IP based firewall rules are specific to source and destination IP addresses and the unique rules and precedence orders assigned. Both IP and non-IP traffic on the same layer 2 interface can be filtered by applying both an IP ACL and a MAC.

A MAC firewall rule uses source and destination MAC addresses for matching operations, where the result is a typical allow, deny or mark designation to packet traffic.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
use [ip-access-list|mac-access-list]

use ip-access-list [in|out] <IP-ACCESS-LIST-NAME> precedence <1-100>

use mac-access-list [in|out] <MAC-ACCESS-LIST-NAME> precedence <1-100>
```

Parameters

```
use ip-access-list [in|out] <IP-ACCESS-LIST-NAME> precedence <1-100>
```

ip-access-list [in|out]	Uses an IP access list with this user role • in – Applies the rule to incoming packets • out – Applies the rule to outgoing packets
<IP-ACCESS-LIST-NAME>	Specify the IP access list name.
precedence <1-100>	After specifying the name of the access list, specify the precedence applied to it. Based on the packets received, a lower precedence value is evaluated first. • <1-100> – Sets a precedence from 1 - 100

```
use mac-access-list [in|out] <MAC-ACCESS-LIST-NAME> precedence <1-100>
```

mac-access-list [in|out]	Uses a MAC access list with this user role • in – Applies the rule to incoming packets • out – Applies the rule to outgoing packets
<MAC-ACCESS-LIST-NAME>	Specify the MAC access list name.
precedence <1-100>	After specifying the name of the access list, specify the precedence applied to it. Based on the packets received, a lower precedence value is evaluated first • <1-100> – Sets a precedence from 1 - 100

Example

```
rfs7000-37FABE(config-role-policy-test-user-role-testing)#use ip-access-list
in
test precedence 9

rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
  ssid not-contains DevUser
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact MotorolaSolutions
  country exact America
  department exact TnV
  emailid exact testing@motorolasolutions.com
```

```
  state exact active
  use ip-access-list in test precedence 9
rfs7000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands:

no	Removes an IP or MAC access list from use with a user role

user-defined

user-role commands

Enables you to define a filter based on an attribute defined in the Active Directory or the OpenLDAP server

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
user-defined <ATTR-STRING> [any|contains|exact|not-contains]

user-defined <ATTR-STRING> [any|contains <WORD>|exact <WORD>|not-contains
<WORD>]
```

Parameters

```
user-defined <ATTR-STRING> [any|exact <WORD>|contains <WORD>|not-contains
<WORD>]
```

user-defined <ATTR-STRING>	Specify a filter based on an attribute defined in the AD or OpenLDAP server. • <ATTR-NAME> – Specify the attribute string. After specifying the attribute name, specify the match type.
any	No specific string to match. This role can be applied to any wireless client. This is the default setting.
contains <WORD>	The role is applied only when the user-defined attribute value, returned by the RADIUS server, contains the string specified in the role. • <WORD> – Specify the string to match (this is case sensitive, and is compared against the value returned by the RADIUS server). It should contain the provided expression.
exact <WORD>	The role is applied only when the user-defined attribute value, returned by the RADIUS server, exactly matches the string specified in the role. • <WORD> – Specify the exact string to match (this is case sensitive, and is compared against the value returned by the RADIUS server). It should be an exact match.
not-contains <WORD>	The role is applied only when the user-defined attribute value, returned by the RADIUS server, does not contain the string specified in the role. • <WORD> – Specify the string not to match (this is case sensitive, and is compared against the value returned by the RADIUS server). It should not contain the provided expression.

Example

```
rfs4000-229D58(config-role-policy-test-user-role-user1)#user-defined
office-location exact EcoSpace
```

```
rfs4000-229D58(config-role-policy-test-user-role-user1)#show context
 user-role user1 precedence 1
  employee-type exact consultant
  user-defined office-location exact EcoSpace
rfs4000-229D58(config-role-policy-test-user-role-user1)#
```

Related Commands:

no	Removes the user-defined filter configured with this user role

Chapter

SMART-RF-POLICY 20

This chapter summarizes *Self Monitoring at Run Time RF* (Smart RF) management policy commands in the CLI command structure.

A Smart RF management policy defines operating and recovery parameters that can be assigned to groups of access points. A Smart RF policy is designed to scan the network to identify the best channel and transmit power for each access point radio.

A Smart RF policy reduces deployment costs by scanning the RF environment to determine the best channel and transmit power configuration for each managed radio. Smart RF policies when applied to specific RF Domains, apply site specific deployment configurations and self-healing values to groups of devices within pre-defined physical RF coverage areas.

Smart RF centralizes the decision process and makes intelligent RF configuration decisions using information obtained from the RF environment. Smart RF helps reduce ongoing management and maintenance costs through the periodic re-calibration of the network. Re-calibration can be initiated manually or can be automatically scheduled to ensure the RF configuration is optimized to factor for RF environment changes (such as new sources of interference, or neighboring access points).

Smart RF also provides self-healing functions by monitoring the network in real-time, and provides automatic mitigation from potentially problematic events such as radio interference, coverage holes and radio failures. Smart RF employs self-healing to enable a WLAN to better maintain wireless client performance and site coverage during dynamic RF environment changes, which typically require manual re-configuration to resolve.

Smart RF is supported on any RF Domain manager. In standalone environments, an individual wireless controller manages the calibration and monitoring phases. In clustered environments, a single wireless controller is elected a Smart RF master and the remaining cluster members operate as Smart RF clients. In cluster operation, the Smart RF master co-ordinates the calibration and configuration and during the monitoring phase receives information from the Smart RF clients.

Before defining a Smart RF policy, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- The Smart RF calibration process impacts associated users and should not be run during business or production hours. The calibration process should be performed during scheduled maintenance intervals or non-business hours.
- For Smart RF to provide effective recovery, RF planning must be performed to ensure overlapping coverage exists at the deployment site. Smart RF can only provide recovery when access points are deployed appropriately. Smart RF is not a solution, it's a temporary measure. Administrators need to determine the root cause of RF deterioration and fix it. Smart RF history/events can assist.

Keep in mind that if a Smart RF managed radio is operating in WLAN mode on a channel requiring DFS, it will switch channels if radar is detected.

- If Smart RF is enabled, the radio picks a channel defined in the Smart RF policy.
- If Smart RF is disabled, but a Smart RF policy is mapped, the radio picks channels specified in the Smart RF policy

- If no SMART RF policy is mapped, the radio selects a random channel

If the radio is a dedicated sensor, it stops termination on that channel if a neighboring access point detect radar. The access point attempts to come back to its original channel (statically configured or selected by Smart RF) after the channel evacuation period has expired.

Change this behavior using the *dfs-rehome* command from the controller or service platform CLI. This keeps the radio on the newly selected channel and prevents the radio from coming back to the original channel, even after the channel evacuation period.

NOTE
Perform RF planning to ensure overlapping coverage exists at a deployment site, for Smart RF to be a viable network performance tool. Smart RF can only provide recovery when access points are deployed appropriately. Smart RF is not a solution, it is a temporary measure. You need to determine the root cause of RF deterioration and fix it. Smart RF history/events can assist in trouble shooting.

Use the (config) instance to configure Smart RF Policy related configuration commands. To navigate to the Smart RF policy instance, use the following commands:

```
<DEVICE>(config)#smart-rf-policy <POLICY-NAME>

rfs7000-37FABE(config)#smart-rf-policy test

rfs7000-37FABE(config-smart-rf-policy-test)#?
Smart RF Mode commands:
  area                    Specify channel list/ power for an area
  assignable-power        Specify the assignable power during power-assignment
  channel-list            Select channel list for smart-rf
  channel-width           Select channel width for smart-rf
  coverage-hole-recovery  Recover from coverage hole
  enable                  Enable this smart-rf policy
  group-by                Configure grouping parameters
  interference-recovery   Recover issues due to excessive noise and
                          interference
  neighbor-recovery       Recover issues due to faulty neighbor radios
  no                      Negate a command or set its defaults
  sensitivity             Configure smart-rf sensitivity (Modifies various
                          other smart-rf configuration items)
  smart-ocs-monitoring    Smart off channel scanning

  clrscr                  Clears the display screen
  commit                  Commit all changes made in this session
  end                     End current mode and change to EXEC mode
  exit                    End current mode and down to previous mode
  help                    Description of the interactive help system
  revert                  Revert changes
  service                 Service Commands
  show                    Show running system information
  write                   Write running configuration to memory or terminal

rfs7000-37FABE(config-smart-rf-policy-test)#
```

smart-rf-policy

SMART-RF-POLICY

Table 18 summarizes Smart RF policy configuration commands.

TABLE 18 Smart-RF-Policy-Config Commands

Command	Description	Reference
area	Configures the channel list and power for a specified area	page 1127
assignable-power	Specifies the power range during power assignment	page 1128
channel-list	Assigns the channel list for the selected frequency	page 1129
channel-width	Selects the channel width for Smart RF configuration	page 1130
coverage-hole-recovery	Enables recovery from errors	page 1131
enable	Enables a Smart RF policy	page 1133
group-by	Configures grouping parameters	page 1133
interference-recovery	Recovers issues due to excessive noise and interference	page 1134
neighbor-recovery	Enables recovery from errors due to faulty neighbor radios	page 1136
no	Negates a command or reverts settings to their default	page 1137
sensitivity	Configures Smart RF sensitivity	page 1139
smart-ocs-monitoring	Applies smart off channel scanning instead of dedicated detectors	page 1140
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

area

smart-rf-policy

Configures the channel list and power for a specified area

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
area <AREA-NAME> channel-list [2.4GHz|5GHz] <CHANNEL-LIST>
```

Parameters

```
area <AREA-NAME> channel-list [2.4GHz|5GHz] <CHANNEL-LIST>
```

area <AREA-NAME>	Specify the area name.
channel-list [2.4GHz|5GHZ] <CHANNEL-LIST>	Selects the channels for the specified area in the 2.4 GHz or 5.0 GHz band • 2.4GHz – Selects the channels for the specified area in the 2.4 GHz band • 5GHz – Selects the channels for the specified area in the 5.0 GHz band The following keyword is common to the 2.4 GHz and 5.0 GHz bands: • <CHANNEL-LIST> – Enter a comma-separated list of channels for the selected band.

Example

```
rfs7000-37FABE(config-smart-rf-policy-test)#area test channel-list 2.4GHz
1,2,3
rfs7000-37FABE(config-smart-rf-policy-test)#

rfs7000-37FABE(config-smart-rf-policy-test)#show context
smart-rf-policy test
 area test channel-list 2.4GHz 1,2,3
rfs7000-37FABE(config-smart-rf-policy-test)#
```

Related Commands:

no	Removes channel list/power configuration for an area

assignable-power

smart-rf-policy

Specifies the power range during power assignment

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
assignable-power [2.4GHz|5GHz] [max|min] <1-20>
```

Parameters

```
assignable-power [2.4GHz|5GHz] [max|min] <1-20>
```

2.4GHz [max|min] <1-20>	Assigns a power range on the 2.4 GHz band • max <1-20> – Sets the upper limit in the range from 1 dBm - 20 dBm (default is 17 dBm) • min <1-20> – Sets the lower limit in the range from 1 dBm - 20 dBm (default is 4 dBm)
5GHz [max|min] <1-20>	Assigns a power range on the 5.0 GHz band • max <1-20> – Sets the upper limit in the range from 1 dBm - 20 dBm (default is 17 dBm) • min <1-20> – Sets the lower limit in the range from 1 dBm - 20 dBm (default is 4 dBm)

Example

```
rfs7000-37FABE(config-smart-rf-policy-test)#assignable-power 5GHz max 20
rfs7000-37FABE(config-smart-rf-policy-test)#assignable-power 5GHz min 8

rfs7000-37FABE(config-smart-rf-policy-test)#show context
smart-rf-policy test
 area test channel-list 2.4GHz 1,2,3
 assignable-power 5GHz min 8
 assignable-power 5GHz max 20
rfs7000-37FABE(config-smart-rf-policy-test)#
```

Related Commands:

no	Resets assignable power to its default

channel-list

smart-rf-policy

Assigns a list of channels, for the selected frequency, used in Smart RF scans

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
channel-list [2.4GHz|5GHz] <WORD>
```

Parameters

```
channel-list [2.4GHz|5GHz] <WORD>
```

2.4GHz <WORD>	Assigns a channel list for the 2.4 GHz band • <WORD> – Specify a comma separated list of channels
5GHz <WORD>	Assigns a channel list for the 5.0 GHz band • <WORD> – Specify a comma separated list of channels

Example

```
rfs7000-37FABE(config-smart-rf-policy-test)#channel-list 2.4Ghz 1,12
```

```
rfs7000-37FABE(config-smart-rf-policy-test)#show context
smart-rf-policy test
 area test channel-list 2.4GHz 1,2,3
 assignable-power 5GHz min 8
 assignable-power 5GHz max 20
 channel-list 2.4GHz 1,12
rfs7000-37FABE(config-smart-rf-policy-test)#
```

Related Commands:

no	Removes the channel list for the selected frequency

channel-width

smart-rf-policy

Selects the channel width for Smart RF configuration

NOTE
In addition to 20 MHz and 40 MHz, AP82XX also provides support for 80 MHz channels.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
channel-width [2.4GHz|5GHz]

channel-width 2.4GHz [20MHz|40MHz|auto]
channel-width 5GHz [20MHz|40MHz|80MHz|auto]
```

Parameters

```
channel-width [2.4GHz|5GHz] [20MHz|40MHz|auto]
```

2.4GHz [20MHz|40MHz|auto]	Assigns the channel width for the 2.4 GHz band • 20MHz – Assigns the 20 MHz channel width. This is the default setting. • 40MHz – Assigns the 40 MHz channel width • auto – Assigns the best possible channel in the 20 MHz or 40 MHz channel width
5GHz [20MHz|40MHz|80MHz|auto]	Assigns the channel width for the 5.0 GHz band • 20MHz – Assigns the 20 MHz channel width • 40MHz – Assigns the 40 MHz channel width. This is the default setting. • auto – Assigns the best possible channel in the 20 MHz, 40 MHz, or 80 MHz channel width

Usage Guidelines:

The 20/40 MHz operation allows the access point to receive packets from clients using 20 MHz, and transmit using 40 MHz. This mode is supported for 11n users on both the 2.4 GHz and 5.0 GHz radios. If an 11n user selects two channels (a primary and secondary channel), the system is configured for dynamic 20/40 operation. When 20/40 is selected, clients can take advantage of wider channels. 802.11n clients experience improved throughput using 40 MHz while legacy clients (either 802.11a or 802.11b/g depending on the radio selected) can still be serviced without interruption using 20 MHz. Select Automatic to enable automatic assignment of channels to working radios to avoid channel overlap and avoid interference from external RF sources.

Example

```
rfs7000-37FABE(config-smart-rf-policy-test)#channel-width 5 auto

rfs7000-37FABE(config-smart-rf-policy-test)#show context
smart-rf-policy test
 area test channel-list 2.4GHz 1,2,3
 assignable-power 5GHz min 8
 assignable-power 5GHz max 20
 channel-list 2.4GHz 1,12
 channel-width 5GHz auto
rfs7000-37FABE(config-smart-rf-policy-test)#
```

Related Commands:

no	Resets channel width for the selected frequency to its default

coverage-hole-recovery

smart-rf-policy

Enables recovery from coverage hole errors detected by Smart RF. Use this command to configure the coverage hole recovery settings.

When coverage hole recovery is enabled, on detection of a coverage hole, Smart RF first determines the power increase needed based on the *signal-to-noise ratio* (SNR) for a client as seen by the access point radio. If a client's SNR is above the specified threshold, the transmit power is increased until the SNR falls below the threshold.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
coverage-hole-recovery
{client-threshold|coverage-interval|interval|snr-threshold}

coverage-hole-recovery {client-threshold [2.4GHz|5GHz] <1-255>}

coverage-hole-recovery {coverage-interval|interval} [2.4GHz|5GHz] <1-120>

coverage-hole-recovery {snr-threshold [2.4Ghz|5Ghz] <1-75>}
```

Parameters

`coverage-hole-recovery {client-threshold [2.4GHz|5GHz] <1-255>}`

client-threshold	Optional. Specifies the minimum number of clients associated to a radio in order to trigger coverage hole recovery.
2.4GHz <1-255>	Specifies the minimum number of clients on the 2.4 GHz band • <1-255> – Sets a value from 1 - 255. The default is 1.
5GHz <1-255>	Specifies the minimum number of clients on the 5.0 GHz band • <1-255> – Sets a value from 1 - 255. The default is 1.

`coverage-hole-recovery {coverage-interval|interval} [2.4GHz|5GHz] <1-120>`

coverage-interval	Optional. Specifies the interval between the discovery of a coverage hole and the initiation of coverage hole recovery
interval	Optional. Specifies the interval at which coverage hole recovery is performed even before a coverage hole is detected
2.4GHz <1-120>	The following keywords are common to the 'coverage-interval' and 'interval' parameters: • 2.4GHz <1-120> – Specifies the coverage hole recovery interval on the 2.4 GHz band • <1-120> – Specify a value from 1 - 120 seconds. **NOTE:** coverage-interval – The default is 10 seconds. **NOTE:** interval – The default is 30 seconds.
5GHz <1-120>	The following keywords are common to the 'coverage-interval' and 'interval' parameters: • 5GHz <1-120> – Specifies a coverage hole recovery interval on the 5.0 GHz band • <1-120> – Specify a value from 1 - 120 seconds. **NOTE:** coverage-interval – The default is 10 seconds. **NOTE:** interval – The default is 30 seconds.

`coverage-hole-recovery {snr-threshold} [2.4Ghz|5Ghz] <1-75>`

snr-threshold	Optional. Specifies the SNR threshold. This value is the SNR threshold for an associated client as seen by its associated AP radio. When the SNR threshold is exceeded, the radio increases its transmit power to increase coverage for the associated client.
2.4GHz <1-75>	Specifies SNR threshold on the 2.4 GHz band • <1-75> – Sets a value from 1 dB - 75 dB. The default is 20 dB.
5GHz <1-75>	Specifies SNR threshold on the 5.0 GHz band • <1-75> – Sets a value from 1 - 75. The default is 20 dB.

Example

```
rfs7000-37FABE(config-smart-rf-policy-test)#coverage-hole-recovery
snr-threshold 5GHz 1

rfs7000-37FABE(config-smart-rf-policy-test)#show context
smart-rf-policy test
 area test channel-list 2.4GHz 1,2,3
 sensitivity custom
 assignable-power 5GHz min 8
 assignable-power 5GHz max 20
 channel-list 2.4GHz 1,12
 channel-width 5GHz auto
 coverage-hole-recovery snr-threshold 5GHz 1
rfs7000-37FABE(config-smart-rf-policy-test)#
```

Related Commands:

no	Disables recovery from coverage hole errors

enable

smart-rf-policy

Enables a Smart RF policy

Use this command to enable this Smart RF policy. Once enabled, the policy can be assigned to a RF Domain supporting a network.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
enable
```

Parameters

None

Example

```
rfs7000-37FABE(config-smart-rf-policy-test)#enable
```

Related Commands:

no	Disables a Smart RF policy

group-by

smart-rf-policy

Enables grouping of APs on the basis of their location in a building (floor) or an area

Within a large RD Domain, grouping of APs (within an area or on the same floor in a building) facilitates statistics gathering and troubleshooting.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
group-by [area|floor]
```

Parameters

```
group-by [area|floor]
```

area	Groups radios based on their area of location
floor	Groups radios based on their floor location Both options are disabled by default.

Example

```
rfs7000-37FABE(config-smart-rf-policy-test)#group-by floor

rfs7000-37FABE(config-smart-rf-policy-test)#show context
smart-rf-policy test
 area test channel-list 2.4GHz 1,2,3
 group-by floor
 sensitivity custom
 assignable-power 5GHz min 8
 assignable-power 5GHz max 20
 channel-list 2.4GHz 1,12
 channel-width 5GHz auto
 coverage-hole-recovery snr-threshold 5GHz 1
rfs7000-37FABE(config-smart-rf-policy-test)#
```

Related Commands:

no	Removes Smart RF group settings

interference-recovery

smart-rf-policy

Enables interference recovery from neighboring radios and other sources of WiFi and non-WiFi interference. Interference is the excess noise detected within the Smart RF supported radio coverage area. Smart RF provides mitigation from interfering sources by monitoring the noise levels and other RF parameters on an access point radio's current channel. When a noise threshold is exceeded, Smart RF selects an alternative channel with less interference. To avoid channel flapping a hold timer is defined, which disables interference avoidance for a specific period of time upon detection. Interference recovery is enabled by default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
interference-recovery
{channel-hold-time|channel-switch-delta|client-threshold|
          interference|neighbor-offset|noise|noise-factor}

interference-recovery {channel-switch-delta [2.4GHz|5GHZ] <5-35>}

interference-recovery {channel-hold-time <0-86400>|client-threshold <1-255>|
          interference|neighbor-offset <3-10>|noise|noise-factor <1.0-3.0>}
```

Parameters

`interference-recovery {channel-switch-delta [2.4GHz|5GHZ] <5-35>}`

channel-switch-delta	Optional. Specifies the difference between the current and best channel interference needed to trigger a channel change. If the difference in noise levels on the current channel and a prospective channel is below the configured threshold, the channel is not changed.
[2.4GHz|5GHz]	Selects the band • 2.4GHz – Selects the 2.4 GHz band • 5GHz – Selects the 5.0 GHz band
<5-35>	Specifies the difference between the current and best channel interference • <5-35> – Sets a value from 5 dBm - 35 dBm. The default setting is 20 dBm for both 2.4 GHz and 5.0 GHz bands.

`interference-recovery {channel-hold-time <0-86400>|client-threshold <1-255>|interference|neighbor-offset <3-10>|noise|noise-factor <1.0-3.0>}`

channel-hold-time <0-86400>	Optional. Defines the minimum time between two channel change recoveries • <0-86400> – Sets the time, in seconds, between channel change assignments based on interference or noise. The default is 7,200 seconds.
client-threshold <1-255>	Optional. Specifies client thresholds needed to avoid channel change. When the threshold number of clients are connected to a radio, the radio avoids changing channels even if the Smart RF master determines that a channel change is required. • <1-255> – Sets the number of clients from 1 - 255. The default is 50.
interference	Optional. Considers external interference values to perform interference recovery. This feature allows the Smart RF policy to scan for excess interference from supported radio devices. WLANs are susceptible to sources of interference, such as neighboring radios, cordless phones, microwave ovens and Bluetooth devices. When interference for WiFi sources is detected, Smart RF supported devices can change the channel and move to a cleaner channel. This feature is enabled by default.
neighbor-offset <3-10>	Optional. Configures a noise factor value, which is taken into consideration when switching channels to avoid interference from neighboring access points. Smart RF enabled access points consider the difference in noise between candidate channels. • <3-10> – Specify a noise factor value from 3 - 10.
noise	Optional. Considers noise values to perform interference recovery. This feature allows the Smart RF policy to scan for excess noise from WiFi devices. When detected, Smart RF supported devices can change their channel and move to a cleaner channel. This feature is enabled by default.
noise-factor <1.0-3.0>	Optional. Configures additional noise factor (the level of network interference detected) for non WiFi interference • <1.0-3.0> – Specify the noise factor from 1.0 - 3.0. The default is 1.50.

Example

```
rfs7000-37FABE(config-smart-rf-policy-test)#interference-recovery
channel-switch-delta 5 5

rfs7000-37FABE(config-smart-rf-policy-test)#show context
```

```
smart-rf-policy test
 area test channel-list 2.4GHz 1,2,3
 group-by floor
 sensitivity custom
 assignable-power 5GHz min 8
 assignable-power 5GHz max 20
 channel-list 2.4GHz 1,12
 channel-width 5GHz auto
 interference-recovery channel-switch-delta 5GHz 5
 coverage-hole-recovery snr-threshold 5GHz 1
rfs7000-37FABE(config-smart-rf-policy-test)#
```

Related Commands:

no	Disables recovery from excessive noise and interference

neighbor-recovery

smart-rf-policy

Enables recovery from errors due to faulty neighboring radios. Enabling neighbor recovery ensures automatic recovery from failed radios within the radio coverage area. Smart RF instructs neighboring access points to increase their transmit power to compensate for the failed radio. Neighbor recovery is enabled by default when the sensitivity setting is medium.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
neighbor-recovery {dynamic-sampling|power-hold-time|power-threshold}

neighbor-recovery {dynamic-sampling} {retries <1-10>|threshold <1-30>}

neighbor-recovery {power-hold-time <0-3600>}

neighbor-recovery {power-threshold [2.4Ghz|5Ghz] <-85--55>}
```

Parameters

```
neighbor-recovery {dynamic-sampling} {retries <1-10>|threshold <1-30>}
```

dynamic-sampling	Optional. Configures dynamic sampling on this Smart RF policy
retries <1-10>	Optional. Specifies the number of retries before allowing a power level adjustments to compensate for a potential coverage hole. • <1-10> – Sets the number of retries from 1 - 10. The default is 3.
threshold <1-30>	Optional. Specifies the minimum number of sample reports before which a power change requires dynamic sampling • <1-30> – Sets the minimum number of reports from 1 - 30. The default is 5.

`neighbor-recovery {power-hold-time <0-3600>}`

power-hold-time	Optional. Specifies the minimum time, in seconds, between two power changes on a radio during neighbor-recovery
<0-3600>	Sets the time from 0 - 3600 sec. The default is 3600 seconds.

`neighbor-recovery {power-threshold [2.4Ghz|5Ghz] <-85--55>}`

power-threshold	Optional. Specifies the power threshold based on the recovery performed The 2.4 GHz/5.0 GHz radio uses as a maximum power increase threshold if the radio is required to increase its output power to compensate for a failed radio within its wireless radio coverage area.
[2.4GHz|5GHz]	Selects the band • 2.4GHz – Selects the 2.4 GHz band • 5GHz – Selects the 5.0 GHz band
<-85--55>	Specify the threshold value • <-85--55> – Sets the power threshold from -85 dBm - -55 dBm. The default is -70 dBm for both the 2.4 GHz and 5.0 GHz bands.

Example

```
rfs7000-37FABE(config-smart-rf-policy-test)#neighbor-recovery power-threshold
2.4 -82
rfs7000-37FABE(config-smart-rf-policy-test)#neighbor-recovery power-threshold
5 -65

rfs7000-37FABE(config-smart-rf-policy-test)#show context
smart-rf-policy test
 area test channel-list 2.4GHz 1,2,3
 group-by floor
 sensitivity custom
 assignable-power 5GHz min 8
 assignable-power 5GHz max 20
 channel-list 2.4GHz 1,12
 channel-width 5GHz auto
 interference-recovery channel-switch-delta 5GHz 5
 neighbor-recovery power-threshold 5GHz -65
 neighbor-recovery power-threshold 2.4GHz -82
 coverage-hole-recovery snr-threshold 5GHz 1
rfs7000-37FABE(config-smart-rf-policy-test)#
```

Related Commands:

no	Disables recovery from faulty neighbor radios

no

smart-rf-policy

Negates a command or sets its default. When used in the config Smart RF policy mode, the no command disables or resets Smart RF settings.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no
[area|assignable-power|channel-list|channel-width|coverage-hole-recovery|enab
le|

group-by|interference-recovery|neighbor-recovery|smart-ocs-monitoring]
```

Parameters

```
no
[area|assignable-power|channel-list|channel-width|coverage-hole-recovery|enab
le|
group-by|interference-recovery|neighbor-recovery|smart-ocs-monitoring]
```

no area	Removes channel list/ power configuration for an area
no assignable-power	Resets assignable power to its default
no auto-assign-sensor	Disables auto assignment of sensor radios to its default
no channel-list	Resets the channel list for the selected frequency to its default
no channel-width	Resets channel width for the selected frequency to its default
no coverage-hole-recovery	Disables recovery from coverage hole errors
no enable	Disables a Smart RF policy
no group-by	Removes a Smart RF policy's group settings
no interference-recovery	Disables recovery from errors due to excessive noise and interference
no neighbor-recovery	Disables recovery from errors due to faulty neighbor radios
no smart-ocs-monitoring	Disables off channel monitoring When used on an AP7161 model access point, this command disables a meshpoint.

Example

```
The following example shows the Smart RF policy 'test' settings before the
'no' commands are executed:
rfs7000-37FABE(config-smart-rf-policy-test)#show context
smart-rf-policy test
 area test channel-list 2.4GHz 1,2,3
 group-by floor
 sensitivity custom
 assignable-power 5GHz min 8
 assignable-power 5GHz max 20
 channel-list 2.4GHz 1,12
 channel-width 5GHz auto
 interference-recovery channel-switch-delta 5GHz 5
 neighbor-recovery power-threshold 5GHz -65
 neighbor-recovery power-threshold 2.4GHz -82
 coverage-hole-recovery snr-threshold 5GHz 1
rfs7000-37FABE(config-smart-rf-policy-test)#
rfs7000-37FABE(config-smart-rf-policy-test)#no interference-recovery
channel-switch-delta 5GHz
rfs7000-37FABE(config-smart-rf-policy-test)#no neighbor-recovery
power-threshold 2.4GHz
```

```
rfs7000-37FABE(config-smart-rf-policy-test)#no neighbor-recovery
power-threshold 5GHz
rfs7000-37FABE(config-smart-rf-policy-test)#no assignable-power 5GHz min
rfs7000-37FABE(config-smart-rf-policy-test)#no assignable-power 5GHz max

The following example shows the Smart RF policy 'test' settings after the 'no'
commands are executed:

rfs7000-37FABE(config-smart-rf-policy-test)#show context
smart-rf-policy test
 area test channel-list 2.4GHz 1,2,3
 group-by floor
 sensitivity custom
 channel-list 2.4GHz 1,12
 channel-width 5GHz auto
 coverage-hole-recovery snr-threshold 5GHz 1
rfs7000-37FABE(config-smart-rf-policy-test)#
```

Related Commands:

area	Specifies the channel list and power for a specified area
assignable-power	Assigns the power range
channel-list	Assigns the channel list for the selected frequency
channel-width	Selects the channel width for Smart RF configuration
coverage-hole-recovery	Enables recovery from coverage hole errors
enable	Enables the configured Smart RF policy features
group-by	Configures grouping parameters on this Smart RF policy
interference-recovery	Enables recovery of errors due to excessive noise and interference
neighbor-recovery	Enables recovery of faulty neighbor radios
smart-ocs-monitoring	Applies smart off channel scanning instead of dedicated detectors

sensitivity

smart-rf-policy

Configures Smart RF sensitivity level. The sensitivity level determines Smart RF scanning and sampling aggressiveness. For example, a low sensitivity level indicates a less aggressive Smart-RF policy. This translates to fewer samples taken during off-channel scanning and short off-channel durations. When the sensitivity level is set to high, Smart-RF collects more samples, and remains off-channel longer.

The Smart RF sensitivity level options include low, medium, high, and custom. Medium, is the default setting. The custom option allows an administrator to adjust the parameters and thresholds for interference recovery, coverage hole recovery, and neighbor recovery. However, the low, medium, and high settings still allow utilization of these features.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
sensitivity [custom|high|low|medium]
```

Parameters

```
sensitivity [custom|high|low|medium]
```

sensitivity	Configures Smart RF sensitivity levels. The options available are: custom, high, low, and medium.
custom	Enables custom interference recovery, coverage hole recovery, and neighbor recovery as additional Smart RF options
high	High sensitivity
low	Low sensitivity
medium	Medium sensitivity. This is the default setting.

Usage Guidelines:

To enable the *power* and *channel setting* parameters, set *sensitivity* to *custom* or *medium*.

To enable the *monitoring* and *scanning* parameters, set *sensitivity* to *custom*.

To enable the *neighbor recovery*, *interference* and *coverage hole recovery* parameters, set *sensitivity* to *custom*.

Example

```
rfs7000-37FABE(config-smart-rf-policy-test)#sensitivity high

rfs7000-37FABE(config-smart-rf-policy-test)#show context
smart-rf-policy test
 area test channel-list 2.4GHz 1,2,3
 group-by floor
 sensitivity high
 channel-list 2.4GHz 1,12
 channel-width 5GHz auto
 smart-ocs-monitoring frequency 5GHz 3
 smart-ocs-monitoring frequency 2.4GHz 3
 smart-ocs-monitoring sample-count 5GHz 3
 smart-ocs-monitoring sample-count 2.4GHz 3

 --More--
rfs7000-37FABE(config-smart-rf-policy-test)#
```

smart-ocs-monitoring

smart-rf-policy

Applies smart *Off Channel Scanning* (OCS) instead of dedicated detectors

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
smart-ocs-monitoring
{awareness-override|client-aware|extended-scan-frequency|

frequency|off-channel-duration|power-save-aware|sample-count|voice-aware}

smart-ocs-monitoring {awareness-override [schedule|threshold]}
smart-ocs-monitoring {awareness-override schedule <1-3> <START-TIME>
<END-TIME> <DAY>}
smart-ocs-monitoring {awareness-override threshold <10-10000>}

smart-ocs-monitoring {client-aware [2.4GHz|5GHz] <1-255>}

smart-ocs-monitoring {extended-scan-frequency [2.4GHz|5GHz] <0-50>}

smart-ocs-monitoring {frequency [2.4GHz|5GHz] <1-120>}

smart-ocs-monitoring {off-channel-duration [2.4GHz|5GHz] <20-150>}

smart-ocs-monitoring {power-save-aware [2.4GHz|5GHz]
[disable|dynamic|strict]}

smart-ocs-monitoring {sample-count [2.4GHz|5GHz] <1-15>}

smart-ocs-monitoring {voice-aware [2.4GHz|5GHz] [disable|dynamic|strict]}
```

Parameters

```
smart-ocs-monitoring {awareness-override schedule <1-3> <START-TIME>
<END-TIME>
<DAY>}
```

awareness-override	Optional. Use this parameter to configure client awareness settings overrides
schedule <1-3> <START-TIME> <END-TIME> {<DAY>}	Configures a time and day schedule when awareness settings are overridden • <1-3> – Sets the awareness override schedule index. A maximum of three overrides can be configured. • <START-TIME> – Sets the override start time in HH:MM format • <END-TIME> – Sets the override end time in HH:MM format • DAY – Optional. Set the day when the override is active. Use one of the following formats: • all – Override is active on all days • sun – Override is active only on Sundays • mon – Override is active only on Mondays • tue – Override is active only on Tuesdays • wed – Override is active only on Wednesdays • thu – Override is active only on Thursdays • fri – Override is active only on Fridays • sat – Override is active only on Saturdays

	`smart-ocs-monitoring {awareness-override threshold <10-10000>}`
awareness-override threshold <10-10000>	Optional. Use this parameter to configure client awareness settings overrides • threshold – Specifies the threshold after which client awareness settings are overridden. When the specified threshold is reached, awareness settings are overridden. • <10-10000> – Specify a threshold value from 10 -10000. The default is 10.

	`smart-ocs-monitoring {client-aware [2.4GHz|5GHz] <1-255>}`
client-aware	Optional. Enables client aware scanning on this Smart RF policy Use this parameter to configure a client threshold number. When the number of clients connected to a radio equals this threshold number, the radio avoids channel scanning. This feature is disabled by default.
2.4GHz <1-255>	Enables client aware scanning on the 2.4 GHz band Avoids radio scanning when a specified minimum number of clients are present • <1-255> – Sets the minimum number of clients from 1 - 255. The default is 1 client.
5GHz <1-255>	Enables client aware scanning on the 5.0 GHz band Avoids radio scanning when a specified minimum number of clients are present • <1-255> – Sets the minimum number of clients from 1 - 255. The default is 1 client.

	`smart-ocs-monitoring {extended-scan-frequency [2.4GHz|5GHz] <0-50>}`
extended-scan-frequency	Optional. Enables an extended scan, as opposed to a neighbor only scan, on this Smart RF policy. This is the frequency radios use to scan for non-peer radios.
2.4GHz <0-50>	Enables extended scan on the 2.4 GHz band • <0-50> – Sets the number of trails from 0 - 50. The default is 5.
5GHz <0-50>	Enables extended scan on the 5.0 GHz band • <0-50> – Sets the number of trails from 0 - 50. The default is 5.

	`smart-ocs-monitoring {frequency [2.4GHz|5GHz] <1-120>}`
frequency	Optional. Specifies the scan frequency. This is the frequency, in seconds, in which smart-ocs-monitoring changes channels for an off channel scan.
2.4GHz <1-120>	Selects the 2.4 GHz band • <1-120> – Sets a scan frequency from 1 - 120 sec. The default is 6 seconds.
5GHz <1-120>	Selects the 5.0 GHz band • <1-120> – Sets a scan frequency from 1 - 120 sec. The default is 6 seconds.

	`smart-ocs-monitoring {off-channel-duration [2.4GHz|5GHz] <20-150>}`
off-channel-duration	Optional. Specifies the duration to scan off channel This is the duration access point radios use to monitor devices within the network and, if necessary, perform self healing and neighbor recovery to compensate for coverage area losses within a RF Domain.
2.4GHz <20-150>	Selects the 2.4 GHz band (in milliseconds) • <20-150> – Sets the off channel duration from 20 - 150 msec. The default is 50 milliseconds.
5GHz <20-150>	Selects the 5.0 GHz band (in milliseconds) • <20-150> – Sets the off channel duration from 20 - 150 msec. The default is 50 milliseconds.

`smart-ocs-monitoring {power-save-aware [2.4GHz|5GHz] [disable|dynamic|strict]}`

power-save-aware	Optional. Enables power save awareness scanning mode on this Smart RF policy. The options are: disable, dynamic, and strict. This setting allows Smart RF to detect power save clients and take them into consideration when performing off channel scans. Strict disables smart monitoring as long as a power save capable client is associated to a radio. Dynamic disables smart monitoring as long as there is data buffered for a power save client at the radio.
2.4GHz [dynamic|strict]	Sets power save awareness scanning mode on the 2.4 GHz band • disable – Disables power save awareness scanning • dynamic – Dynamically avoids scanning based on traffic for power save (PSP) clients • strict – Strictly avoids scanning when PSP clients are present The default is dynamic.
5GHz [dynamic|strict]	Sets power save awareness scanning mode on the 5.0 GHz band • disable – Disables power save awareness scanning • dynamic – Dynamically avoids scanning based on traffic for PSP clients • strict – Strictly avoids scanning when PSP clients are present The default is dynamic.

`smart-ocs-monitoring {sample-count [2.4GHz|5GHz] <1-15>}`

sample-count	Optional. Specifies the number of samples to collect before reporting an issue to the Smart RF master
2.4GHz <1-15>	Selects the 2.4 GHz band • <1-15> – Specifies the number of samples to collect from 1 - 15. The default is 10.
5GHz <1-15>	Selects the 5.0 GHz band • <1-15> – Specifies the number of samples to collect from 1 - 15. The default is 5.

`smart-ocs-monitoring {voice-aware [2.4GHz|5GHz] [disable|dynamic|strict]}`

voice-aware	Optional. Enables voice awareness scanning mode on this Smart RF policy. The options are: disable, dynamic, and strict. Strict disables smart monitoring as long as a voice client is associated to a radio. Dynamic disables smart monitoring as long as there is data buffered for a voice client at the radio.
2.4GHz [dynamic|strict]	Specifies the scanning mode on the 2.4 GHz band • disable – Disables voice awareness scanning • dynamic – Dynamically avoids scanning based on traffic for voice clients • strict – Strictly avoids scanning when voice clients are present **NOTE:** The default is dynamic.
5GHz [dynamic|strict]	Specifies the scanning mode on the 5.0 GHz band • dynamic – Dynamically avoids scanning based on traffic for voice clients • strict – Strictly avoids scanning when voice clients are present. **NOTE:** The default is dynamic.

Example

```
rfs7000-37FABE(config-smart-rf-policy-test)#smart-ocs-monitoring
extended-scan-frequency 2.4Ghz 9
rfs7000-37FABE(config-smart-rf-policy-test)#smart-ocs-monitoring sample-count
2.4Ghz 3

rfs7000-37FABE(config-smart-rf-policy-test)#show context
smart-rf-policy test
 area test channel-list 2.4GHz 1,2,3
 group-by floor
```

```
 sensitivity custom
 channel-list 2.4GHz 1,12
 channel-width 5GHz auto
 smart-ocs-monitoring off-channel-duration 2.4GHz 25
 smart-ocs-monitoring frequency 5GHz 3
 smart-ocs-monitoring frequency 2.4GHz 3
 smart-ocs-monitoring sample-count 5GHz 3
 smart-ocs-monitoring sample-count 2.4GHz 3
 smart-ocs-monitoring extended-scan-frequency 5GHz 0
 smart-ocs-monitoring extended-scan-frequency 2.4GHz 9
 root-recovery root-path-metric-threshold 800
--More--
rfs7000-37FABE(config-smart-rf-policy-test)#
```

Related Commands:

no	Disables off channel monitoring

Chapter

WIPS-POLICY

21

This chapter summarizes the *Wireless Intrusion Protection Systems* (WIPS) policy commands in the CLI command structure.

WIPS is an additional measure of security designed to continuously monitor the network for threats and intrusions. Along with wireless VPNs, encryptions, and authentication policies WIPS enhances the security of a WLAN.

The WIPS policy enables detection of intrusions and threats that a managed network is likely to encounter. However, the WIPS policy does not include threat mitigation configurations. These intrusions and threats are available within the WIPS policy configuration mode as pre configured, fixed events. Each event consists of a set of frames or anomalies that may be harmful to the managed network. You can enable/disable various aspects of each individual event.

Events are broadly grouped into the following three categories:

- Excessive/Thresholdable events: These events detect DOS attacks, like excessive deauths, EAP floods etc. Threshold limits for such events can be configured for *mobile units* (MU) and radios. Once these threshold limits are exceeded, an event is triggered. Stations triggering an event are usually filtered. You can configure a filter ageout specifying the time for which the station, triggering the event, is filtered. However, the filter ageout only applies when the MU-threshold is exceeded. When radio threshold is reached, the system raises a warning about the same and updates event history with event details.
- Station/MU anomalies: These events are triggered when a MU performs suspicious activities that can compromise the security and stability of the managed network. You can configure a filter ageout, similar to the above class of events, to filter the station triggering such events.
- AP/neighbor anomalies: These events are triggered when an AP or neighbor sends suspicious frames. The system cannot filter APs or neighbors triggering such events. However, the system warns you about such attacks, allowing you to take further actions against such APs and neighbors.

In addition to event monitoring configuration, the WIPS policy also you to configure a list of signatures. Unlike events, signatures are not fixed. You are free to define your own signatures based on a specific set of parameters. A signature is a rule, consisting of a set of fields to match and a corresponding set of actions in case of a match. By default, whenever a signature is matched an event log is triggered. This event log is similar to the one triggered upon an event. In addition to an event log, you can also configure other actions. Signatures have all the features supported by events. In fact most events are internally implemented as signatures.

Signature rules are of the following three types:

- ssid, ssid length rule: This signature matches a specified SSID or SSID length. It is mandatory to configure the frame type to match for this signature. When configured, only frame types allowed are beacons, probe requests, and probe responses. Example rule: ssid : AirJack and frame type beacon : Signature for AirJack attack.
- payload rule: This signature matches a particular payload at a particular frame offset. You can restrict these matches based on frame type. Example rule: Payload : 0x00601d Offset 3 : Netstumbler

- address-match rule: This signature matches one or more address fields. The address fields supported are BSSID, source-MAC, and destination-MAC. You can also specify frame types to match. The frame types supported are assoc, auth, beacon, data, deauth, disassoc, mgmt, probe-request, and probe-response.

A WIPS policy, once configured, has to be attached to a RF Domain to take effect. Multiple WIPS policies can be configured at the same time, but only one policy can be attached to a given RF Domain at any time.

NOTE
To attach a WIPS policy to a RF Domain, in the RF Domain configuration mode, execute the *use* > *wips-policy* <*WIPS-POLICY-NAME*> command. For more information, see *use*.

Use the (config) instance to configure WIPS policy commands. To navigate to the WIPS policy instance, use the following commands:

```
<DEVICE>(config)#wips-policy <POLICY-NAME>

rfs7000-37FABE(config)#wips-policy test
rfs7000-37FABE(config-wips-policy-test)#?
Wips Policy Mode commands:
  br-detection               Rogue AP detection
  enable                     Enable this wips policy
  event                      Configure an event
  history-throttle-duration  Configure the duration for which event duplicates
                             are not stored in history
  interference-event         Specify events which will contribute to smart-rf
                             wifi interference calculations
  no                         Negate a command or set its defaults
  signature                  Signature to configure
  use                        Set setting to use

  clrscr                     Clears the display screen
  commit                     Commit all changes made in this session
  do                         Run commands from Exec mode
  end                        End current mode and change to EXEC mode
  exit                       End current mode and down to previous mode
  help                       Description of the interactive help system
  revert                     Revert changes
  service                    Service Commands
  show                       Show running system information
  write                      Write running configuration to memory or terminal

rfs7000-37FABE(config-wips-policy-test)#
```

wips-policy

WIPS-POLICY

Table 19 summarizes WIPS policy configuration commands.

TABLE 19 WIPS-Policy-Config Commands

Command	Description	Reference
br-detection	Defines the WIPS AP detection configuration	page 1147
enable	Enables a WIPS policy	page 1148

TABLE 19 WIPS-Policy-Config Commands

Command	Description	Reference
event	Configures events	page 1149
history-throttle-duration	Configures the duration event duplicates are omitted from the event history	page 1152
interference-event	Specifies events contributing to the Smart RF WiFi interference calculations	page 1153
no	Negates a command or sets its default	page 1154
signature	Configures a WIPS policy signature and enters its configuration mode	page 1158
use	Defines a WIPS policy settings	page 1171
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

br-detection

wips-policy

Enables the detection of unauthorized or unsanctioned APs. Unauthorized APs are untrusted access points connected to an access point managed network. These untrusted APs accept wireless client associations. It is important to detect such rogue APs and declare them unauthorized.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
br-detection {ageout|wait-time}
br-detection {age-out <30-86400>|wait-time <10-600>}
```

Parameters

```
br-detection {age-out <30-86400>|wait-time <10-600>}
```

age-out <30-86400>	Optional. Configures the unauthorized AP ageout interval. The WIPS policy uses this value to ageout unauthorized APs. • <30-86400> – Sets an ageout interval from 30 - 86400 seconds. The default is 5 minutes (300 seconds).
wait-time <10-600>	Optional. Configures the wait time before a detected AP is declared as unauthorized and potentially removed • <10-600> – Sets a wait time from 10 - 600 seconds. The default is 1 minute (60 seconds).

Example

```
rfs7000-37FABE(config-wips-policy-test)#br-detection wait-time 15
rfs7000-37FABE(config-wips-policy-test)#br-detection age-out 50

rfs7000-37FABE(config-wips-policy-test)#show context
wips-policy test
 br-detection-ageout 50
 br-detection-wait-time 15
rfs7000-37FABE(config-wips-policy-test)#
```

Related Commands:

no	Resets unauthorized or unsanctioned AP detection settings to default

enable

wips-policy

Enables this WIPS policy

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
enable
```

Parameters

None

Example

```
rfs7000-37FABE(config-wips-policy-test)#enable
rfs7000-37FABE(config-wips-policy-test)#
```

Related Commands:

no	Disables a WIPS policy

event

wips-policy

Configures events, filters and threshold values for this WIPS policy. Events are grouped into three categories, AP anomaly, client anomaly, and excessive. WLANs are baselined for matching criteria. Any deviation from this baseline is considered an anomaly and logged as an event.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
event [br-anomaly|client-anomaly|enable-all-events|excessive]

event br-anomaly
[ad-hoc-violation|airjack|br-ssid-broadcast-in-beacon|asleap|

impersonation-attack|null-probe-response|transmitting-device-using-invalid-ma
c|
          unencrypted-wired-leakage|wireless-bridge]

event client-anomaly [dos-broadcast-deauth|fuzzing-all-zero-macs|

fuzzing-invalid-frame-type|fuzzing-invalid-mgmt-frames|fuzzing-invalid-seq-nu
m|

identical-src-and-dest-addr|invalid-8021x-frames|netstumbler-generic|
          non-conforming-data|tkip-mic-counter-measures|wellenreiter]
{filter-ageout <0-86400>}

event enable-all-events

event excessive
[80211-replay-check-failure|aggressive-scanning|auth-server-failures|
          decryption-failures|dos-assoc-or-auth-flood|dos-eapol-start-storm|

dos-unicast-deauth-or-disassoc|eap-flood|eap-nak-flood|frames-from-unassoc-st
ation]
          {filter-ageout <0-86400>|threshold-client <0-65535>|threshold-radio
<0-65535>}
```

Parameters

```
event br-anomaly
[ad-hoc-violation|airjack|br-ssid-broadcast-in-beacon|asleap|
impersonation-attack|null-probe-response|transmitting-device-using-invalid-ma
c|
unencrypted-wired-leakage|wireless-bridge]
```

br-anomaly	Enables AP anomaly event tracking An AP anomaly event refers to suspicious frames sent by neighboring APs. An administrator enables or disables the filtering of each listed event and sets the thresholds for the generation of event notification and filtering.
ad-hoc-violation	Tracks ad-hoc network violations
airjack	Tracks AirJack attacks
br-ssid-broadcast-in-beacon	Tracks AP SSID broadcasts in beacon events
asleap	Tracks ASLEAP attacks. These attacks break *Lightweight Extensible Authentication Protocol* (LEAP) passwords
impersonation-attack	Tracks impersonation attacks. These are also referred to as spoofing attacks, where the attacker assumes the address of an authorized device.
null-probe-response	Tracks null probe response attacks
transmitting-device-using-invalid-mac	Tracks the transmitting device using an invalid MAC attacks
unencrypted-wired-leakage	Tracks unencrypted wired leakage
wireless-bridge	Tracks *wireless bridge* (WDS) frames

```
event client-anomaly
[dos-broadcast-deauth|fuzzing-all-zero-macs|fuzzing-invalid-frame-type|fuzzin
g-invalid-mgmt-frames|fuzzing-invalid-seq-num|identical-src-and-dest-addr|inv
alid-8021x-frames|netstumbler-generic|non-conforming-data|wellenreiter]
{filter-ageout <0-86400>}
```

client-anomaly	Enables client anomaly event tracking These are suspicious events performed by wireless clients compromising the security of the network. An administrator can enable or disable filtering of each listed event and set the thresholds required for the generation of the event notification and filtering action applied.
dos-broadcast-deauth	Tracks DoS broadcast deauthentication events
fuzzing-all-zero-macs	Tracks Fuzzing: All zero MAC addresses observed
fuzzing-invalid-frame-type	Tracks Fuzzing: Invalid frame type detected
fuzzing-invalid-mgmt-frames	Tracks Fuzzing: Invalid management frame detected
fuzzing-invalid-seq-num	Tracks Fuzzing: Invalid sequence number detected
identical-src-and-dest-addr	Tracks identical source and destination addresses detection
invalid-8021x-frames	Tracks Fuzzing: Invalid 802.1x frames detected
netstumbler-generic	Tracks Netstumbler (v3.2.0, 3.2.3, 3.3.0) events
non-conforming-data	Tracks non conforming data packets

wellenreiter	Tracks Wellenreiter events
filter-ageout <0-86400>	The following keywords are common to all of the above client anomaly events: • filter-ageout <0-86400> – Optional. Configures the filter expiration interval in seconds • <0-86400> – Sets the filter ageout interval from 0 - 86400 seconds. The default is 0 seconds. **NOTE:** For each violation define a filter time in seconds, which determines how long the packets (received from an attacking device) are ignored once a violation has been triggered. Ignoring frames from an attacking device minimizes the effectiveness of the attack and the impact to the site until permanent mitigation can be performed. The filter ageout value is applicable across the entire RF Domain using this WIPS policy. If an MU is detected performing an attack and is filtered by one of the APs, the information is passed on to all APs and controllers within the RF Domain through the domain manager. Consequently the MU is filtered, for the specified period of time, across all devices.

`event enable-all-events`

enable-all-events	Enables tracking of all intrusion events (client anomaly and excessive events)

`event excessive [80211-replay-check-failure|aggressive-scanning|auth-server-failures| decryption-failures|dos-assoc-or-auth-flood|dos-eapol-start-storm |dos-unicast-deauth-or-disassoc|eap-flood|eap-nak-flood|frames-from-unassoc-station]` *`{filter-ageout [<0-86400>]|threshold-client [<0-5535>]|threshold-radio <0-65535>}`*

excessive	Enables the tracking of excessive events. Excessive events are actions performed continuously and repetitively. These events can impact the performance of the controller managed network. DoS attacks come under this category.
80211-replay-check-failure	Tracks 802.11replay check failure
aggressive-scanning	Tracks aggressive scanning events
auth-server-failures	Tracks failures reported by authentication servers
decryption-failures	Tracks decryption failures
dos-assoc-or-auth-flood	Tracks DoS association or authentication floods
dos-eapol-start-storm	Tracks DoS EAPOL start storms
dos-unicast-deauth-or-disassoc	Tracks DoS dissociation or deauthentication floods
eap-flood	Tracks EAP floods
eap-nak-flood	Tracks EAP NAK floods
frames-from-unassoc-station	Tracks frames from unassociated clients
filter-ageout <0-86400>	The following keywords are common to all excessive events: • filter-ageout <0-86400> – Optional. Configures a filter expiration interval in seconds. It sets the duration for which the client is filtered. The client is added to a ACL as a special entry and frames received from this client are dropped. • <0-86400> – Sets a filter ageout interval from 0 - 86400 seconds. The default is 0 seconds. **NOTE:** This value is applicable across the RF Domain. If a client is detected performing an attack and is filtered by one of the APs, the information is passed to the domain controller. The domain controller then propagates this information to all APs and wireless controllers in the RF Domain.

threshold-client <0-65535>	The following keywords are common to all excessive events: • threshold-client <0-65535> – Optional. Configures a client threshold value after which the filter is triggered and an event is recorded • <0-65535> – Sets a wireless client threshold value from 0 - 65535 seconds
threshold-radio <0-65535>	The following keywords are common to all excessive events: • threshold-radio <0-65535> – Optional. Configures a radio threshold value after which the filter is triggered and an event is recorded • <0-65535> – Sets a radio threshold value from 0 - 65535 seconds

Example

```
rfs7000-37FABE(config-wips-policy-test)#event excessive
80211-replay-check-failure filter-ageout 9 threshold-client 8 threshold-radio
99

rfs7000-37FABE(config-wips-policy-test)#show context
wips-policy test
 event excessive 80211-replay-check-failure threshold-client 10
threshold-radio 99 filter-ageout 9
 event client-anomaly wellenreiter filter-ageout 99
 br-detection-ageout 50
 br-detection-wait-time 15
rfs7000-37FABE(config-wips-policy-test)#
```

Related Commands:

no	Disables WIPS policy events tracking

history-throttle-duration

wips-policy

Configures the duration event duplicates are omitted from the event history

The system maintains a history of all events that have occurred, on each device, within a RF Domain. Sometimes an event occurs for a prolonged period of time and tends to fill up the event history list. In such a scenario, duplicate information added to the event history list can be throttled for a specified period of time. Once this period is over, duplicate entries are once again allowed.

Event history statistics are periodically sent to the domain manager, which can be queried to ascertain the general health of the domain.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
history-throttle-duration <30-86400>
```

Parameters

```
history-throttle-duration <30-86400>
```

history-throttle-duration <30-86400>	Configures the duration event duplicates are omitted from the event history • <30-86400> – Sets a value from 30 - 86400 seconds. The default is 120 seconds.

Example

```
rfs7000-37FABE(config-wips-policy-test)#history-throttle-duration 77

rfs7000-37FABE(config-wips-policy-test)#show context
wips-policy test
 history-throttle-duration 77
 event excessive 80211-replay-check-failure threshold-client 10
threshold-radio 99 filter-ageout 9
 event client-anomaly wellenreiter filter-ageout 99
 br-detection-ageout 50
 br-detection-wait-time 15
rfs7000-37FABE(config-wips-policy-test)#
```

Related Commands:

no	Resets the history throttle duration to its default (120 seconds)

interference-event

wips-policy

Specifies events contributing to the Smart RF WiFi interference calculations

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
interference-event [non-conforming-data|wireless-bridge]
```

Parameters

```
interference-event [non-conforming-data|wireless-bridge]
```

non-conforming-data	Considers non conforming data packets when calculating Smart RF interference
wireless-bridge	Considers Wireless Bridge (WDS) frames when calculating Smart RF interference

Example

```
rfs7000-37FABE(config-wips-policy-test)#interference-event
non-conforming-data

rfs7000-37FABE(config-wips-policy-test)#show context
wips-policy test
 history-throttle-duration 77
```

```
 event excessive 80211-replay-check-failure threshold-client 10
threshold-radio 99 filter-ageout 9
 event client-anomaly wellenreiter filter-ageout 99
 interference-event non-conforming-data
 br-detection-ageout 50
 br-detection-wait-time 15
rfs7000-37FABE(config-wips-policy-test)#
```

Related Commands:

no	Disables this WIPS policy signature as a Smart RF interference source

no

wips-policy

Negates a command or resets configured settings to their default. When used in the config WIPS policy mode, the no command negates or resets filters and thresholds.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no [br-detection|enable|event|history-throttle-duration|interference-event|
           signature|use]

no [enable|history-throttle-duration]

no br-detection {ageout|wait-time} {<LINE-SINK>}

no event [br-anomaly|client-anomaly|enable-all-events|excessive]

no event br-anomaly
[ad-hoc-violation|airjack|br-ssid-broadcast-in-beacon|asleap|

impersonation-attack|null-porbe-response|transmitting-device-using-invalid-ma
c|
           unencrypted-wired-leakage|wireless-bridge]

no event client-anomaly [dos-broadcast-deauth|fuzzing-all-zero-macs|

fuzzing-invalid-frame-type|fuzzing-invalid-mgmt-frames|fuzzing-invalid-seq-nu
m|

identical-src-and-dest-addr|invalid-8021x-frames|netstumbler-generic|
           non-conforming-data|wellenreiter] {filter-ageout <0-86400>}
```

```
no event excessive [80211-replay-check-failure|aggressive-scanning|
          auth-server-failures|decryption-failures|dos-assoc-or-auth-flood|

dos-eapol-start-storm|dos-unicast-deauth-or-disassoc|eap-flood|eap-nak-flood|
          frames-from-unassoc-station] {filter-ageout
<0-86400>|threshold-client <0-65535>|
          threshold-radio <0-65535>}

no interference-event [non-conforming-data|wireless-bridge]

no signature <WIPS-SIGNATURE>

no use device-categorization
```

Parameters

```
no [enable|history-throttle-duration]
```

no enable	Disables a WIPS policy from use with a profile
no history-throttle-duration	Resets the history throttle duration to its default (120 seconds). This is the duration event duplicates are omitted from the event history.

```
no br-detection {ageout|wait-time} {<LINE-SINK>}
```

no br-detection	Disables the detection of unauthorized or unsanctioned APs
ageout <LINE-SINK>	Optional. Resets a rogue device's ageout interval to its default (300 seconds)
wait-time <LINE-SINK>	Optional. Resets the wait time value to its default (60 seconds)

```
no event br-anomaly
[ad-hoc-violation|airjack|br-ssid-broadcast-in-beacon|asleap|
impersonation-attack|null-porbe-response|transmitting-device-using-invalid-ma
c|
unencrypted-wired-leakage|wireless-bridge]
```

no event	Disables WIPS policy event tracking
br-anomaly	Disables AP anomaly event tracking
ad-hoc-violation	Disables ad-hoc network violation event tracking
airjack	Disables the tracking of AirJack attacks
br-ssid-broadcast-in-beacon	Disables the tracking of AP SSID broadcasts in beacon events
asleap	Disables the tracking of ASLEAP attacks
impersonation-attack	Disables the tracking of impersonation attacks
null-probe-response	Disables the tracking of null probe response attacks
transmitting-device-using-invalid-mac	Disables the tracking of invalid device MAC addresses
unencrypted-wired-leakage	Disables the tracking of unencrypted wired leakage detection
wireless-bridge	Disables the tracking of wireless bridge frames

```
no event client-anomaly
[dos-broadcast-deauth|fuzzing-all-zero-macs|fuzzing-invalid-frame-type|fuzzin
g-invalid-mgmt-frames|fuzzing-invalid-seq-num|identical-src-and-dest-addr|inv
alid-8021x-frames|netstumbler-generic|non-conforming-data|wellenreiter]
{filter-ageout <0-86400>}
```

no event	Disables WIPS policy event tracking
client-anomaly	Disables client anomaly event tracking
dos-broadcast-deauth	Disables DoS broadcast deauthentication event tracking
fuzzing-all-zero-macs	Disables Fuzzing tracking: All zero MAC addresses observed
fuzzing-invalid-frame-type	Disables Fuzzing tracking: Invalid frame type detected
fuzzing-invalid-mgmt-frames	Disables Fuzzing tracking: Invalid management frame
fuzzing-invalid-seq-num	Disables Fuzzing tracking: Invalid sequence number
identical-src-and-dest-addr	Disables the tracking of identical source and destination addresses
invalid-8021x-frames	Disables Fuzzing tracking: Invalid 802.1x frames
netstumbler-generic	Disables Netstumbler (v3.2.0, 3.2.3, 3.3.0) event tracking
non-conforming-data	Disables non conforming data packet tracking
wellenreiter	Disables Wellenreiter event tracking
filter-ageout <0-86400>	The following keywords are common to all client anomaly events: • Optional. Resets the filter expiration interval in seconds • <0-86400> – Resets a filter ageout interval from 0 - 86400 seconds

```
no event excessive [80211-replay-check-failure|aggressive-scanning|
auth-server-failures|decryption-failures|dos-assoc-or-auth-flood|dos-eapol-st
art-storm|
dos-unicast-deauth-or-disassoc|eap-flood|eap-nak-flood|frames-from-unassoc-st
ation] {filter-ageout <0-86400>|threshold-client <0-65535>|threshold-radio
<0-65535>}
```

no event	Disables WIPS policy event tracking
excessive	Disables the tracking of excessive events. Excessive events consist of actions that are performed continuously and repetitively.
80211-replay-check-failure	Disables the tracking of 802.11 replay check failure
aggressive-scanning	Disables aggressive scanning event tracking
auth-server-failures	Disables the tracking of failures reported by authentication servers
decryption-failures	Disables the tracking of decryption failures
dos-assoc-or-auth-flood	Disables DoS association or authentication flood tracking
dos-eapol-start-storm	Disables the tracking of DoS EAPOL start storms
dos-unicast-deauth-or-disassoc	Disables DoS disassociation or deauthentication flood tracking
eap-flood	Disables the tracking of EAP floods
eap-nak-flood	Disables the tracking of EAP NAKfloods
frames-from-unassoc-station	Disables the tracking of frames from unassociated clients
filter-ageout <0-86400>	Optional. Resets the filter expiration interval in seconds. It resets the duration for which a client is filtered. The client is added to a ACL as a special entry and frames received from this client are dropped. • <0-86400> – Resets a filter ageout interval from 0 - 86400 seconds

threshold-client <0-65535>	Optional. Resets a client threshold limit after which the filter is triggered and an event is recorded • <0-65535> – Resets a wireless client threshold limit from 0 - 65535 seconds
threshold-radio <0-65535>	Optional. Resets a radio threshold limit after which an event is recorded • <0-65535> – Resets a radio threshold limit from 0 - 65535 seconds

```
no interference-event [non-conforming-data|wireless-bridge]
```

no interference-event	Disables interference event settings
non-conforming-data	Does not consider non conforming data packets when calculating Smart RF interference
wireless-bridge	Does not consider Wireless Bridge frames when calculating Smart RF interference

```
no signature <WIPS-SIGNATURE>
```

no signature	Deletes a WIPS policy signature
<WIPS-SIGNATURE>	Defines the unique name given to a WIPS policy signature

```
no use device-categorization
```

no use	Disables the use of a device categorization policy with this WIPS policy
device-categorization	Resets the device categorization name to its default

Usage Guidelines:

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
The following example shows the WIPS Policy ‘test’ settings before the ‘no’
commands are executed:

rrfs7000-37FABE(config-wips-policy-test)#show context
wips-policy test
 history-throttle-duration 77
 event excessive 80211-replay-check-failure threshold-client 10
threshold-radio 99 filter-ageout 9
 event client-anomaly wellenreiter filter-ageout 99
 interference-event non-conforming-data
 br-detection-ageout 50
 br-detection-wait-time 15
rfs7000-37FABE(config-wips-policy-test)#

rfs7000-37FABE(config-wips-policy-test)#no event client-anomaly wellenreiter
filter-ageout 99
rfs7000-37FABE(config-wips-policy-test)#no interference-event
non-conforming-data
rfs7000-37FABE(config-wips-policy-test)#no history-throttle-duration

The following example shows the WIPS Policy ‘test’ settings after the ‘no’
commands are executed:

rfs7000-37FABE(config-wips-policy-test)#show context
wips-policy test
 event excessive 80211-replay-check-failure threshold-client 10
threshold-radio 99 filter-ageout 9
 no event client-anomaly wellenreiter filter-ageout 99
 br-detection-ageout 50
 br-detection-wait-time 15
```

```
rfs7000-37FABE(config-wips-policy-test)#
```

Related Commands:

br-detection	Enables the detection of unauthorized or unsactioned access points
enable	Enables a WIPS policy for use with a profile
event	Configures events, filters, and threshold values for a WIPS policy
history-throttle-duration	Configures the duration event duplicates are omitted from the event history
interference-event	Specifies events contributing to the Smart RF WiFi interference calculations
signature	Configures a WIPS policy signature
use	Enables the categorization of devices on this WIPS policy

signature

wips-policy

Attack and intrusion patterns are identified and configured as signatures in a WIPS policy. The WIPS policy compares packets in the network with pre configured signatures to identify threats.

The following table summarizes WIPS policy signature configuration commands.

signature	Configures a WIPS policy signature and enters its configuration mode	page 1158
signature mode commands	Summarizes WIPS signature configuration mode commands	page 1159

signature

signature

Configures a WIPS policy signature

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
signature <SIGNATURE-NAME>
```

Parameters

```
signature <SIGNATURE-NAME>
```

signature <SIGNATURE-NAME>	Configures a WIPS policy signature • <SIGNATURE-NAME> – Enter a name for the WIPS policy signature. The name should not exceed 64 characters.

Example

```
rfs7000-37FABE(config-wips-policy-test)#signature test
rfs7000-37FABE(config-test-signature-test)

rfs7000-37FABE(config-test-signature-test)#?
Wips Signature Mode commands:
  bssid               Bssid mac address
  dst-mac             Destination mac address
  filter-ageout       Configure filter ageout
  frame-type          Configure frame-type to match
  interference-event  Signature is a smart-rf interference source
  mode                Enable/Disable signature
  no                  Negate a command or set its defaults
  payload             Configure a payload
  src-mac             Source mac address
  ssid-match          Match based on ssid
  threshold-client    Configure client threshold limit
  threshold-radio     Configure radio threshold limit

  clrscr              Clears the display screen
  commit              Commit all changes made in this session
  do                  Run commands from Exec mode
  end                 End current mode and change to EXEC mode
  exit                End current mode and down to previous mode
  help                Description of the interactive help system
  revert              Revert changes
  service             Service Commands
  show                Show running system information
  write               Write running configuration to memory or terminal

rfs7000-37FABE(config-test-signature-test)#

rfs7000-37FABE(config-wips-policy-test)#show context
wips-policy test
 event excessive 80211-replay-check-failure threshold-client 10
threshold-radio 99 filter-ageout 9
 no event client-anomaly wellenreiter filter-ageout 99
 signature test
  interference-event
  bssid 11-22-33-44-55-66
  dst-mac 55-66-77-88-99-00
  frame-type reassoc
  filter-ageout 8
  threshold-client 88
  payload 1 pattern brocade offset 1
 br-detection-ageout 50
 br-detection-wait-time 15
rfs7000-37FABE(config-wips-policy-test)#
```

Related Commands:

no	Deletes a WIPS policy signature

signature mode commands

signature

The following table summarizes WIPS policy signature configuration mode commands.

Commands	Description	Reference
bssid	Configures the BSSID MAC address	page 1160
dst-mac	Configures the destination MAC address	page 1161
filter-ageout	Configures the filter ageout interval	page 1162
frame-type	Configures the frame type used for matching	page 1162
interference-event	Configures this WIPS policy signature as the Smart RF interference source	page 1163
mode	Enables or disables the signature mode	page 1164
payload	Configures payload settings	page 1165
src-mac	Configures the source MAC address	page 1165
ssid-match	Configures a match based on SSID	page 1166
threshold-client	Configures the wireless client threshold limit	page 1167
threshold-radio	Configures the radio threshold limit	page 1168
no	Negates a command or sets its default	page 1169
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

bssid

signature mode commands

Configures a BSSID MAC address with this WIPS signature for matching

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
bssid <MAC>
```

Parameters

```
bssid <MAC>
```

bssid <MAC>	Configures a BSSID MAC address to match • <MAC> – Specify the MAC address.

Example

```
rfs7000-37FABE(config-test-signature-test)#bssid 11-22-33-44-55-66

rfs7000-37FABE(config-test-signature-test)#show context
signature test
bssid 11-22-33-44-55-66
rfs7000-37FABE(config-test-signature-test)#
```

Related Commands:

no	Disables a WIPS signature BSS ID

dst-mac

signature mode commands

Configures a destination MAC address for the packet examined for matching

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
dst-mac <MAC>
```

Parameters

```
dst-mac <MAC>
```

dst-mac <MAC>	Configures a destination MAC address to match • <MAC> – Specify the destination MAC address.

Example

```
rfs7000-37FABE(config-test-signature-test)#dst-mac 55-66-77-88-99-00

rfs7000-37FABE(config-test-signature-test)#show context
signature test
  bssid 11-22-33-44-55-66
  dst-mac 55-66-77-88-99-00
rfs7000-37FABE(config-test-signature-test)#
```

Related Commands:

no	Disables a WIPS signature destination MAC address

filter-ageout

signature mode commands

Configures the filter ageout interval in seconds. This is the duration a client, triggering a WIPS event, is excluded from RF Domain manager radio association.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
filter-ageout <1-86400>
```

Parameters

```
filter-ageout <1-86400>
```

filter-ageout <1-86400>	Configures the filter ageout interval from 1 - 86400 seconds

Example

```
rfs7000-37FABE(config-test-signature-test)#filter-ageout 8

rfs7000-37FABE(config-test-signature-test)#show context
 signature test
  bssid 11-22-33-44-55-66
  dst-mac 55-66-77-88-99-00
  filter-ageout 8
rfs7000-37FABE(config-test-signature-test)#
```

Related Commands:

no	Removes the configured filter ageout interval

frame-type

signature mode commands

Configures the frame type used for matching with this WIPS policy signature

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
frame-type
[all|assoc|auth|beacon|data|deauth|disassoc|mgmt|probe-req|probe-resp|
          reassoc]
```

Parameters

```
frame-type
[all|assoc|auth|beacon|data|deauth|disassoc|mgmt|probe-req|probe-resp|
reassoc]
```

frame-type	Configures the frame type used for matching
all	Configures all frame type matching
assoc	Configures association frame matching
auth	Configures authentication frame matching
beacon	Configures beacon frame matching
data	Configures data frame matching
deauth	Configures deauthentication frame matching
disassoc	Configures disassociation frame matching
mgmt	Configures management frame matching
probe-req	Configures probe request frame matching
probe-resp	Configures probe response frame matching
reassoc	Configures re-association frame matching

Usage Guidelines:

The frame type configured determines the SSID match type configured. To configure the SSID match type as SSID, the frame type must be beacon, probe-req or probe-resp.

Example

```
rfs7000-37FABE(config-test-signature-test)#frame-type reassoc

rfs7000-37FABE(config-test-signature-test)#show context
 signature test
  bssid 11-22-33-44-55-66
  dst-mac 55-66-77-88-99-00
  frame-type reassoc
  filter-ageout 8
rfs7000-37FABE(config-test-signature-test)#
```

Related Commands:

no	Resets a WIPS signature frame type

interference-event

signature mode commands

Configures this WIPS policy signature as Smart RF interference source

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
interference-event
```

Parameters

None

Example

```
rfs7000-37FABE(config-test-signature-test)#interference-event

rfs7000-37FABE(config-test-signature-test)#show context
 signature test
  interference-event
  bssid 11-22-33-44-55-66
  dst-mac 55-66-77-88-99-00
  frame-type reassoc
  filter-ageout 8
rfs7000-37FABE(config-test-signature-test)#
```

Related Commands:

no	Disables this WIPS policy signature as Smart RF interference source

mode

signature mode commands

Enables or disables a WIPS policy signature

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
mode enable
```

Parameters

```
mode enable
```

mode enable	Enables this WIPS signature

Example

```
rfs7000-37FABE(config-test-signature-test)#mode enable
rfs7000-37FABE(config-test-signature-test)#
```

Related Commands:

no	Disables a WIPS signature

payload

signature mode commands

Configures payload settings. The payload command sets a numerical index pattern and offset for this WIPS signature.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
payload <1-3> pattern <WORD> offset <0-255>
```

Parameters

```
payload <1-3> pattern <WORD> offset <0-255>
```

payload <1-3>	Configures payload settings • <1-3> – Sets the payload index
pattern <WORD>	Specifies the pattern to match: hex or string • <WORD> – Sets the pattern name
offset <0-255>	Specifies the payload offset to start the pattern match • <0-255> – Sets the offset value

Example

```
rfs7000-37FABE(config-test-signature-test)#payload 1 pattern brocade offset 1

rfs7000-37FABE(config-test-signature-test)#show context
 signature test
  bssid 11-22-33-44-55-66
  dst-mac 55-66-77-88-99-00
  frame-type assoc
  filter-ageout 8
  payload 1 pattern brocade offset 1
rfs7000-37FABE(config-test-signature-test)#
```

Related Commands:

no	Removes payload and associated settings

src-mac

signature mode commands

Configures a source MAC address for a packet examined for matching

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
src-mac <MAC>
```

Parameters

```
src-mac <MAC>
```

src-mac <MAC>	Configures the source MAC address to match • <MAC> – Specify the source MAC address.

Example

```
rfs7000-37FABE(config-test-signature-test)#src-mac 00-1E-E5-EA-1D-60

rfs7000-37FABE(config-test-signature-test)#show context
 signature test
  bssid 11-22-33-44-55-66
  src-mac 00-1E-E5-EA-1D-60
  dst-mac 55-66-77-88-99-00
  frame-type assoc
  filter-ageout 8
  payload 1 pattern brocade offset 1
rfs7000-37FABE(config-test-signature-test)#
```

Related Commands:

no	Removes a WIPS signature source MAC address

ssid-match

signature mode commands

Configures the SSID (and its character length) used for matching

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
ssid-match [ssid|ssid-len]

ssid-match [ssid <SSID>|ssid-len <0-32>]
```

Parameters

```
ssid-match [ssid <SSID>|ssid-len <0-32>]
```

ssid <SSID>	Specifies the SSID match string • <SSID> – Specify the SSID string. **NOTE:** Specify the correct SSID to ensure proper filtering.
ssid-len <0-32>	Specifies the length of the SSID • <0-32> – Specify the SSID length from 0 - 32 characters.

Example

```
rfs7000-37FABE(config-test-signature-test)#ssid-match ssid PrinterLan

rfs7000-37FABE(config-test-signature-test)#show context
 signature test
  bssid 11-22-33-44-55-66
  src-mac 00-1E-E5-EA-1D-60
  dst-mac 55-66-77-88-99-00
  frame-type beacon
  ssid-match ssid PrinterLan
  filter-ageout 8
  payload 1 pattern brocade offset 1
rfs7000-37FABE(config-test-signature-test)#
```

Related Commands:

no	Removes the configured SSID

threshold-client

signature mode commands

Configures the wireless client threshold limit. When the wireless client exceeds the specified limit, an event is triggered.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
threshold-client <1-65535>
```

Parameters

```
threshold-client <1-65535>
```

threshold-client <1-65535>	Configures the wireless client threshold limit • <1-65535> – Sets the threshold limit for a 60 second window from 1 - 65535

Example

```
rfs7000-37FABE(config-test-signature-test)#threshold-client 88
```

```
rfs7000-37FABE(config-test-signature-test)#show context
 signature test
  bssid 11-22-33-44-55-66
  src-mac 00-1E-E5-EA-1D-60
  dst-mac 55-66-77-88-99-00
  frame-type beacon
  ssid-match ssid PrinterLan
  filter-ageout 8
  threshold-client 88
  payload 1 pattern brocade offset 1
rfs7000-37FABE(config-test-signature-test)#
```

Related Commands:

no	Removes the wireless client threshold limit configured with a WIPS policy signature

threshold-radio

signature mode commands

Configures the radio's threshold limit. When the radio exceeds the specified limit, an event is triggered.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
threshold-radio <1-65535>
```

Parameters

```
threshold-radio <1-65535>
```

threshold-radio <1-65535>	Configures the radio's threshold limit • <1-65535> – Specify the threshold limit for a 60 second window from 1 - 65535.

Example

```
rfs7000-37FABE(config-test-signature-test)#threshold-radio 88

rfs7000-37FABE(config-test-signature-test)#show context
 signature test
  bssid 11-22-33-44-55-66
  src-mac 00-1E-E5-EA-1D-60
  dst-mac 55-66-77-88-99-00
  frame-type beacon
  ssid-match ssid PrinterLan
  filter-ageout 8
  threshold-client 88
  threshold-radio 88
  payload 1 pattern brocade offset 1
```

```
rfs7000-37FABE(config-test-signature-test)#
```

Related Commands:

no	Removes the radio's threshold limit configured with a WIPS policy signature

no

signature mode commands

Negates a command or resets settings to their default. When used in the config WIPS policy signature mode, the no command resets or removes WIPS signature settings.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no
[bssid|dst-mac|filter-ageout|frame-type|interference-event|mode|payload|src-m
ac|
          ssid-match|threshold-client|threshold-radio]

no [bssid|dts-mac|filter-ageout|frame-type|interference-event|mode enable|
          payload <1-3>|src-mac|ssid-match
[ssid|ssid-len]|threshold-client|threshold-radio]
```

Parameters

```
no [bssid|dst-mac|filter-ageout|frame-type|interference-event|mode enable|
payload <1-3>|src-mac|ssid-match
[ssid|ssid-len]|threshold-client|threshold-radio]
```

no bssid	Disables a WIPS signature BSS ID
no dst-mac	Disables a WIPS signature destination MAC address
no filter-ageout	Removes the filter ageout interval. This is the duration a client, triggering a WIPS event, is excluded from RF Domain manager radio association.
no frame-type	Removes a WIPS signature frame type
no interference-event	Disables this WIPS policy signature as a Smart RF interference source
no mode enable	Disables a WIPS signature • enable – Changes the mode from enabled to disabled
no payload <1-3>	Removes payload index and associated settings. The payload command sets a numerical index pattern and offset for this WIPS signature • <1-3> – Sets the payload index
no src-mac	Removes a WIPS signature source MAC address
no ssid-match [ssid|ssid-len]	Removes the configured SSID and the SSID character length • ssid – Removes the specified SSID match string • ssid-len – Removes the specified character length of the SSID

no threshold-client	Removes the wireless client threshold limit configured with a WIPS policy. When the wireless client exceeds the specified limit, an event is triggered.
no threshold-radio	Removes a radio threshold limit configured with a WIPS policy. When the radio exceeds the specified threshold limit, an event is triggered.

Usage Guidelines:

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
The following is the WIPS signature ‘test’ settings before the execution of
the ‘no’ command:

rfs7000-37FABE(config-test-signature-test)#show context
 signature test
  bssid 11-22-33-44-55-66
  src-mac 00-1E-E5-EA-1D-60
  dst-mac 55-66-77-88-99-00
  frame-type beacon
  ssid-match ssid PrinterLan
  filter-ageout 8
  threshold-client 88
  threshold-radio 88
  payload 1 pattern brocade offset 1
rfs7000-37FABE(config-test-signature-test)#

The following is the WIPS signature ‘test’ settings after the execution of the
‘no’ command:

rfs7000-37FABE(config-test-signature-test)#no mode enable
rfs7000-37FABE(config-test-signature-test)#no bssid
rfs7000-37FABE(config-test-signature-test)#no dst-mac
rfs7000-37FABE(config-test-signature-test)#no src-mac
rfs7000-37FABE(config-test-signature-test)#no filter-ageout
rfs7000-37FABE(config-test-signature-test)#no threshold-client
rfs7000-37FABE(config-test-signature-test)#no threshold-radio

rfs7000-37FABE(config-test-signature-test)#
 signature test
  no mode enable
  frame-type beacon
  payload 1 pattern brocade offset 1
rfs7000-37FABE(config-test-signature-test)
```

Related Commands:

bssid	Configures a WIPS signature BSSID MAC address
dst-mac	Configures a destination MAC address for the packet examined for matching
filter-ageout	Configures the filter ageout interval
frame-type	Configures the frame type to match with a signature
interference-event	Specifies events contributing to the Smart RF WiFi interference calculations
mode	Enables or disables a WIPS signature

payload	Configures payload settings. The payload command sets a numerical index pattern and offset for this WIPS signature.
src-mac	Configures a source MAC address for the packet examined for matching
ssid-match	Configures a SSID for matching
threshold-client	Configures a wireless client threshold limit
threshold-radio	Configures a radio threshold limit

use

wips-policy

Enables device categorization on this WIPS policy. This command uses an existing device categorization list. The list categorizes devices as authorized or unauthorized.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
use device-categorization <DEVICE-CATEGORIZATION>
```

Parameters

```
use device-categorization <DEVICE-CATEGORIZATION>
```

device-categorization <DEVICE-CATEGORIZATION>	Configures a device categorization list • <DEVICE-CATEGORIZATION> – Specify the device categorization object name to associate with this profile

Example

```
rfs7000-37FABE(config-wips-policy-test)#use device-categorization test

rfs7000-37FABE(config-wips-policy-test)#show context
wips-policy test
 event excessive 80211-replay-check-failure threshold-client 10
threshold-radio 99 filter-ageout 9
 no event client-anomaly wellenreiter filter-ageout 99
 signature test
  interference-event
  bssid 11-22-33-44-55-66
  dst-mac 55-66-77-88-99-00
  frame-type reassoc
  filter-ageout 8
  threshold-client 88
  payload 1 pattern brocade offset 1
 br-detection-ageout 50
 br-detection-wait-time 15
 use device-categorization test
rfs7000-37FABE(config-wips-policy-test)#
```

Related Commands:

no	Disables the use of a device categorization policy with a WIPS policy

Chapter

WLAN-QOS-POLICY

22

This chapter summarizes the WLAN QoS policy in the CLI command structure.

A WLAN QoS policy increases network efficiency by prioritizing data traffic. Prioritization reduces congestion. This is essential because of the lack of bandwidth for all users and applications. QoS helps ensure each WLAN on the wireless controller receives a fair share of the overall bandwidth, either equally or as per the proportion configured. Packets directed towards clients are classified into categories such as Video, Voice and Data. Packets within each category are processed based on the weights defined for each WLAN

Each WLAN QoS policy has a set of parameters which it groups into categories, such as management, voice and data. Packets within each category are processed based on the weights defined for each WLAN.

Use the (config) instance to configure WLAN QoS policy commands. To navigate to the WLAN QoS policy instance, use the following commands:

```
<DEVICE>(config)#wlan-qos-policy <POLICY-NAME>

rfs7000-37FABE(config)#wlan-qos-policy test
rfs7000-37FABE(config-wlan-qos-test)#?
WLAN QoS Mode commands:
  accelerated-multicast  Configure accelerated multicast streams address and
                         forwarding QoS classification
  classification         Select how traffic on this WLAN must be classified
                         (relative prioritization on the radio)
  multicast-mask         Egress multicast mask (frames that match bypass the
                         PSPqueue. This permits intercom mode operation
                         without delay even in the presence of PSP clients)
  no                     Negate a command or set its defaults
  qos                    Quality of service
  rate-limit             Configure traffic rate-limiting parameters on a
                         per-wlan/per-client basis
  svp-prioritization     Enable spectralink voice protocol support on this wlan
  voice-prioritization   Prioritize voice client over other client (for
                         non-WMM clients)
  wmm                    Configure 802.11e/Wireless MultiMedia parameters
  clrscr                 Clears the display screen
  commit                 Commit all changes made in this session
  do                     Run commands from Exec mode
  end                    End current mode and change to EXEC mode
  exit                   End current mode and down to previous mode
  help                   Description of the interactive help system
  revert                 Revert changes
  service                Service Commands
  show                   Show running system information
  write                  Write running configuration to memory or terminal
rfs7000-37FABE(config-wlan-qos-test)#
```

22

wlan-qos-policy

WLAN-QOS-POLICY

WLAN QoS configurations differ significantly from QoS policies configured for radios. WLAN QoS configurations are designed to support the data requirements of wireless clients, including the data types they support and their network permissions. Radio QoS policies are specific to the transmit and receive characteristics of the connected radio's themselves, independent from the wireless clients these access point radios support.

Table 20 summarizes WLAN QoS policy configuration commands.

TABLE 20 WLAN-QoS-Policy-Config Commands

Command	Description	Reference
accelerated-multicast	Configures accelerated multicast stream addresses and forwards QoS classifications	page 1174
classification	Classifies WLAN traffic based on priority	page 1175
multicast-mask	Configures the egress prioritization multicast mask	page 1177
no	Negates a command or sets its default	page 1178
qos	Defines the QoS configuration	page 1180
rate-limit	Configures the WLAN traffic rate limit using a WLAN QoS policy	page 1181
svp-prioritization	Enables Spectralink voice protocol support on a WLAN	page 1184
voice-prioritization	Prioritizes voice client over other clients	page 1185
wmm	Configures 802.11e/wireless multimedia parameters	page 1185
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

accelerated-multicast

wlan-qos-policy

Configures the accelerated multicast stream address and forwarding QoS classification settings

Enabling this option allows the system to automatically detect and convert multicast streams to unicast streams. When a stream is converted and queued up for transmission, there are a number of classification mechanisms that can be applied to the stream. Use the classification options to specify the traffic type to prioritize.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
accelerated-multicast [<IP>|autodetect]

accelerated-multicast [<IP>|autodetect] {classification
[background|best-effort|trust|
          video|voice]}
```

Parameters

```
accelerated-multicast [<IP>|autodetect] {classification
[background|best-effort|
trust|video|voice]}
```

accelerated-multicast	Configures the accelerated multicast stream address and forwarding QoS classification
<IP>	Configures a multicast IP address in the A.B.C.D format. The system can configure up to 32 IP addresses for each WLAN QoS policy
autodetect	Allows the system to automatically detect multicast streams to be accelerated. This parameter allows the system to convert multicast streams to unicast, or to specify multicast streams converted to unicast.
classification	Optional. Configures the QoS classification (traffic class) settings. When the stream is converted and queued for transmission, specify the type of classification applied to the stream. The options are: background, best-effort, trust, voice, and video.
background	Forwards streams with background (low) priority. This parameter is common to both <IP> and auto detect.
best-effort	Forwards streams with best effort (normal) priority. This parameter is common to both <IP> and autodetect.
trust	No change to the streams forwarding traffic class. This parameter is common to both <IP> and autodetect.
video	Forwards streams with video traffic priority. This parameter is common to both <IP> and autodetect.
voice	Forwards streams with voice traffic priority. This parameter is common to both <IP> and autodetect.

Example

```
rfs7000-37FABE(config-wlan-qos-test)#accelerated-multicast autodetect
classification voice

rfs7000-37FABE(config-wlan-qos-test)#show context
wlan-qos-policy test
 qos trust dscp
 qos trust wmm
 accelerated-multicast autodetect classification voice
rfs7000-37FABE(config-wlan-qos-test)#
```

classification

wlan-qos-policy

Specifies how traffic on this WLAN is classified. This classification is based on relative prioritization on the radio.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
classification [low|non-unicast|non-wmm|normal|video|voice|wmm]

classification [low|normal|video|voice|wmm]

classification non-unicast [voice|video|normal|low|default]

classification non-wmm [voice|video|normal|low]
```

Parameters

`classification [low|normal|video|voice|wmm]`

low	Optimized for background traffic. Implies all traffic on this WLAN is low priority on the radio
normal	Optimized for best effort traffic. Implies all traffic on this WLAN is prioritized as best effort traffic on the radio
video	Optimized for video traffic. Implies all traffic on this WLAN is prioritized as video traffic on the radio
voice	Optimized for voice traffic. Implies all traffic on this WLAN is prioritized as voice traffic on the radio
wmm	Uses WMM based classification, using DSCP or 802.1p tags, to classify traffic into different queues Implies WiFi Multimedia QoS extensions are enabled on this radio. This allows different traffic streams between the wireless client and the access point to be prioritized according to the type of traffic (voice, video etc). The WMM classification supports high throughput data rates required for 802.11n device support.

`classification non-unicast [voice|video|normal|low|default]`

non-unicast	Optimized for non-unicast traffic. Implies all traffic on this WLAN is designed for broadcast or multiple destinations
video	Optimized for non-unicast video traffic. Implies all WLAN non-unicast traffic is classified and treated as video packets
voice	Optimized for non-unicast voice traffic. Implies all WLAN non-unicast traffic is classified and treated as voice packets
normal	Optimized for non-unicast best effort traffic. Implies all WLAN non-unicast traffic is classified and treated as normal priority packets (best effort)
low	Optimized for non-unicast background traffic. Implies all WLAN non-unicast traffic is classified and treated as low priority packets (background)
default	Uses the default classification mode (same as unicast classification if WMM is disabled, normal if unicast classification is WMM)

```
classification non-wmm [voice|video|normal|low]
```

non-wmm	Specifies how traffic from non-WMM clients is classified
voice	Optimized for non-WMM voice traffic. Implies all WLAN non-WMM client traffic is classified and treated as voice packets
video	Optimized for non-WMM video traffic. Implies all WLAN non-WMM client traffic is classified and treated as video packets
normal	Optimized for non-WMM best effort traffic. Implies all WLAN non-WMM client traffic is classified and treated as normal priority packets (best effort)
low	Optimized for non-WMM background traffic. Implies all WLAN non-WMM client traffic is classified and treated as low priority packets (background)

Example

```
rfs7000-37FABE(config-wlan-qos-test)#classification wmm

rfs7000-37FABE(config-wlan-qos-test)#classification non-wmm video

rfs7000-37FABE(config-wlan-qos-test)#classification non-unicast normal

rfs7000-37FABE(config-wlan-qos-test)#show context
wlan-qos-policy test
 classification non-wmm video
 classification non-unicast normal
 qos trust dscp
 qos trust wmm
 accelerated-multicast autodetect classification voice
rfs7000-37FABE(config-wlan-qos-test)#
```

multicast-mask

wlan-qos-policy

Configures an egress prioritization multicast mask for this WLAN QoS policy

Normally all multicast and broadcast packets are buffered until the periodic DTIM interval (indicated in the 802.11 beacon frame), when clients in power save mode wake to check for frames. However, for certain applications and traffic types, the administrator may want the frames transmitted immediately, without waiting for the DTIM interval. By configuring a primary or secondary prioritization multicast mask, the network administrator can indicate which packets are transmitted immediately.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
multicast-mask [primary|secondary] <MAC/MASK>
```

Parameters

```
multicast-mask [primary|secondary] <MAC/MASK>
```

primary <MAC/MASK>	Configures the primary egress prioritization multicast mask • <MAC/MASK> – Sets the MAC address and the mask in the AA-BB-CC-DD-EE-FF/XX-XX-XX-XX-XX-XX-XX format **NOTE:** Setting masks is optional and only needed if there are traffic types requiring special handling.
secondary <MAC/MASK>	Configures the primary egress prioritization multicast mask • <MAC/MASK> – Sets the MAC address and the mask in the AA-BB-CC-DD-EE-FF / XX-XX-XX-XX-XX-XX-XX format

Example

```
rfs7000-37FABE(config-wlan-qos-test)#multicast-mask primary
11-22-33-44-55-66/22-33-44-55-66-77

rfs7000-37FABE(config-wlan-qos-test)#show context
wlan-qos-policy test
 classification non-wmm video
 multicast-mask primary 11-22-33-44-55-66/22-33-44-55-66-77
 classification non-unicast normal
 qos trust dscp
 qos trust wmm
 accelerated-multicast autodetect classification voice
rfs7000-37FABE(config-wlan-qos-test)#
```

no

wlan-qos-policy

Negates a command or resets settings to their default

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no [accelerated-multicast|classification|multicast-mask|qos|rate-limit|
          svp-prioritization|voice-prioritization|wmm]

no [accelerated-multicast [<IP>|autodetect]|classification
{non-unicast|non-wmm}|
          multicast-mask [primary|secondary]|qos trust
[dscp|wmm]|svp-prioritization|
          voice-prioritization]

no rate-limit [client|wlan] [from-air|to-air]
{max-burst-size|rate|red-threshold}
no rate-limit [client|wlan] [from-air|to-air] {max-burst-size|rate|
          red-threshold [background|best-effort|video|voice]}

no wmm [background|best-effort|power-save|qbss-load-element|video|voice]
no wmm [power-save|qbss-load-element]
```

```
no wmm [backgorund|best-effort|video|voice] [aifsn|cw-max|cw-min|txop-limit]
```

Parameters

```
no [accelerated-multicast [<IP>|autodetect]|classification
{non-unicast|non-wmm}|
multicast-mask [primary|secondary]|qos trust [dscp|wmm]|svp-prioritization|
voice-prioritization]
```

no accelerated-multicast [<IP>|autodetect]	Disables accelerated multicast streams and forwarding QoS classification • <IP> – Removes specified IP address. Specify the IP address • autodetect – Disables multicast streams automatic detection
no classification [non-unicast| non-wmm]	Disables WLAN classification scheme • non-unicast – Optional. Removes multicast and broadcast packet classification • non-wmm – Optional. Removes non-WMM client traffic classification
no multicast-mask [primary|secondary]	Disables the egress prioritization primary or secondary multicast mask • primary – Removes the first egress multicast mask • secondary – Removes the second egress multicast mask
no qos trust [disquiet]	Disables the QoS service • trust – Ignores the trust QOS values of ingressing packets • dscp – Ignores the IP DSCP values of ingressing packets • wmm – Ignores the 802.11 WMM QoS values of ingressing packets
no svp-prioritization	Disables *Spectralink Voice Protocol* (SVP) support on a WLAN
no voice-prioritization	Disables voice client priority over other clients (applies to non-WMM clients)

```
no rate-limit [client|wlan] [from-air|to-air] {max-burst-size|rate|
red-threshold [background|best-effort|video|voice]}
```

no rate-limit [client|wlan]	Disables traffic rate limit parameters • Disables client traffic rate limits • Disables WLAN traffic rate limits
[from-air|to-air]	The following are common to the client and WLAN parameters: • from-air – Removes client/WLAN traffic rate limits in the up link direction. This is traffic from the wireless client to the network • to-air – Removes client/WLAN traffic rate limits in the down link direction. This is traffic from the network to the wireless client
max-burst-size	Optional. Disables the maximum burst size value
rate	Optional. Disables the traffic rates configured for a wireless client or WLAN
red-threshold	Optional. Disables random early detection threshold values configured for the traffic class • background – Disables the low priority traffic (background) threshold value • best-effort – Disables the normal priority traffic (best effort) threshold value • video – Disables the video traffic threshold value • voice – Disables the voice traffic threshold value

```
no wmm [power-save|qbss-load-element]
```

no wmm	Disables 802.11e/wireless multimedia parameters
power-save	Disables support for WMM-Powersave (U-APSD)
qbss-load-element	Disables support for the QBSS load information element in beacons and probe responses

`no wmm [backgorund|best-effort|video|voice] [aifsn|cw-max|cw-min|txop-limit]`

no wmm	Disables 802.11e/wireless multimedia parameters
background	Disables background access category parameters
best-effort	Disables best effort access category parameters
video	Disables video access category parameters
voice	Disables voice access category parameters

Example

```
The following example shows the WLAN QoS Policy ‘test’ settings before the
‘no’ commands are executed:

rfs7000-37FABE(config-wlan-qos-test)#show context
wlan-qos-policy test
 classification non-wmm video
 multicast-mask primary 11-22-33-44-55-66/22-33-44-55-66-77
 classification non-unicast normal
 qos trust dscp
 qos trust wmm
 accelerated-multicast autodetect classification voice
rfs7000-37FABE(config-wlan-qos-test)#

rfs7000-37FABE(config-wlan-qos-test)#no classification non-wmm
rfs7000-37FABE(config-wlan-qos-test)#no multicast-mask primary
rfs7000-37FABE(config-wlan-qos-test)#no qos trust dscp

The following example shows the WLAN QoS Policy ‘test’ settings after the ‘no’
commands are executed:

rfs7000-37FABE(config-wlan-qos-test)#show context
wlan-qos-policy test
 classification non-unicast normal
 no qos trust dscp
 qos trust wmm
 accelerated-multicast autodetect classification voice
rfs7000-37FABE(config-wlan-qos-test)#
```

Related Commands:

accelerated-multicast	Configures the accelerated multicast streams address and forwards the QoS classification
classification	Classifies WLAN traffic based on priority
multicast-mask	Configures the egress prioritization multicast mask
qos	Defines the QoS configuration
rate-limit	Configures a WLAN’s traffic rate limits
svp-prioritization	Enables Spectralink voice protocol support on a WLAN
voice-prioritization	Prioritizes voice client over other clients
wmm	Configures the 802.11e/wireless multimedia parameters

qos

wlan-qos-policy

Enables QoS on this WLAN

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
qos trust [dscp|wmm]
```

Parameters

```
qos trust [dscp|wmm]
```

trust [dscp|wmm]	Trusts the QoS values of ingressing packets • dscp – Trusts the IP DSCP values of ingressing packets • wmm – Trusts the 802.11 WMM QoS values of ingressing packets

Example

```
rfs7000-37FABE(config-wlan-qos-test)#qos trust wmm
rfs7000-37FABE(config-wlan-qos-test)#qos trust dscp

rfs7000-37FABE(config-wlan-qos-test)#show context
wlan-qos-policy test
 classification non-unicast normal
 qos trust dscp
 qos trust wmm
 accelerated-multicast autodetect classification voice
rfs7000-37FABE(config-wlan-qos-test)#
```

rate-limit

wlan-qos-policy

Configures the WLAN traffic rate limits using the WLAN QoS policy

Excessive traffic causes performance issues or brings down the network entirely. Excessive traffic can be caused by numerous sources including network loops, faulty devices or malicious software such as a worm or virus that has infected one or more devices at the branch. Rate limiting limits the maximum rate sent to or received from the wireless network (and WLAN) per wireless client. It prevents any single user from overwhelming the wireless network. It can also provide differential service for service providers. The uplink and downlink rate limits are usually configured on a RADIUS server using Brocade vendor specific attributes. Rate limits are extracted from the RADIUS server's response. When such attributes are not present, settings defined on the controller (access point, wireless controller, or service platform) are applied. An administrator can set separate QoS rate limits for upstream (data transmitted from the managed network) and downstream (data transmitted to the managed network traffic.

Before defining rate limit thresholds for WLAN upstream and downstream traffic, Brocade recommends you define the normal number of ARP, broadcast, multicast and unknown unicast packets that typically transmit and receive from each supported WMM access category. If thresholds are defined too low, normal network traffic (required by end-user devices) are dropped resulting in intermittent outages and performance problems.

Connected wireless clients can also have QoS rate limit settings defined in both the upstream and downstream direction.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
rate-limit [client|wlan] [from-air|to-air]
{max-burst-size|rate|red-threshold}

rate-limit [client|wlan] [from-air|to-air] {max-burst-size <2-1024>|rate
<50-1000000>}

rate-limit [client|wlan] [from-air|to-air] {red-threshold [background <0-100>|
          best-effort <0-100>|video <0-100>|voice <0-100>]}
```

Parameters

```
rate-limit [client|wlan] [from-air|to-air] {max-burst-size <2-1024>|rate
<50-1000000>}
```

rate-limit	Configures traffic rate limit parameters
client	Configures traffic rate limiting parameters on a per-client basis
wlan	Configures traffic rate limiting parameters on a per-WLAN basis
from-air	Configures traffic rate limiting from a wireless client to the network
to-air	Configures the traffic rate limit from the network to a wireless client
max-burst-size <2-1024>	Optional. Sets the maximum burst size from 2 - 1024 kbytes. The chances of the upstream or downstream packet transmission getting congested for the WLAN's client destination are reduced for smaller burst sizes. The default is 320 kbytes. **NOTE:** Smaller the burst, lesser are the chances of upstream packet transmission resulting in congestion for the WLAN's client destinations. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should then add a 10% margin (minimally) to allow for traffic bursts at the site.
rate <50-1000000>	Optional. Sets the traffic rate from 50 - 1000000 kbps. This limit is the threshold value for the maximum number of packets received or transmitted over the WLAN from all access categories. Any traffic that exceeds the specified rate is dropped and a log message is generated. The default is 5000 kbps.

```
rate-limit [client|wlan] [from-air|to-air] {red-threshold [background <0-100>|
best-effort <0-100>|video <0-100>|voice <0-100>]}
```

rate-limit	Configures traffic rate limit parameters
client	Configures traffic rate limiting parameters on a per-client basis
wlan	Configures traffic rate limiting parameters on a per-WLAN basis
from-air	Configures traffic rate limiting from a wireless client to the network
to-air	Configures the traffic rate limit from the network to a wireless client
red-threshold	Configures random early detection threshold values for a designated traffic class
background <0-100>	The following is common to the 'from-air' and 'to-air' parameters: Optional. Sets a percentage value for background traffic in the upstream or downstream direction. Background traffic exceeding the defined threshold is dropped and a log message is generated. The default threshold is 50% for traffic in both directions.
best-effort <0-100>	The following is common to the 'from-air' and 'to-air' parameters: Optional. Sets a percentage value for best effort traffic in the upstream or downstream direction. Best effort traffic exceeding the defined threshold is dropped and a log message is generated. The default threshold is 50% for traffic in both directions.
video <0-100>	The following is common to the 'from-air' and 'to-air' parameters: Optional. Sets a percentage value for video traffic in the upstream or downstream direction. Video traffic exceeding the defined threshold is dropped and a log message is generated. The default threshold is 25% fro traffic in both directions.
voice <0-100>	The following is common to the 'from-air' and 'to-air' parameters: Optional. Sets a percentage value for voice traffic in the upstream or downstream direction. Voice traffic exceeding the defined threshold is dropped and a log message is generated. The default threshold is 0% for traffic in both directions. 0% means no early random drops will occur.

Usage Guidelines:

The following information should be taken into account when configuring rate limits:

- Background traffic consumes the least bandwidth, so this value can be set to a lower value once a general downstream rate is known by the network administrator (using a time trend analysis).
- Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general upstream rate is known by the network administrator (using a time trend analysis).
- Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis).
- Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis).

Example

```
rfs7000-37FABE(config-wlan-qos-test)#rate-limit wlan from-air max-burst-size 6

rfs7000-37FABE(config-wlan-qos-test)#rate-limit wlan from-air rate 55

rfs7000-37FABE(config-wlan-qos-test)#rate-limit wlan from-air red-threshold
best-effort 10
rfs7000-37FABE(config-wlan-qos-test)#rate-limit client from-air red-threshold
background 3

rfs7000-37FABE(config-wlan-qos-test)#show context
```

```
wlan-qos-policy test
 classification non-wmm video
 multicast-mask primary 11-22-33-44-55-66/22-33-44-55-66-77
 classification non-unicast normal
 rate-limit wlan from-air rate 55
 rate-limit wlan from-air max-burst-size 6
 rate-limit wlan from-air red-threshold best-effort 10
 rate-limit client from-air red-threshold background 3
 qos trust dscp
 qos trust wmm
 accelerated-multicast autodetect classification voice
rfs7000-37FABE(config-wlan-qos-test)#
```

svp-prioritization

wlan-qos-policy

Enables WLAN SVP support on this WLAN QoS policy. SVP support enables the identification and prioritization of traffic from Spectralink/Ploycomm phones. This gives priority to voice, with voice management packets supported only on certain legacy Brocade VOIP phones. If the wireless client classification is WMM, non-WMM devices recognized as voice devices have all their traffic transmitted at voice priority. Devices are classified as voice, when they emit SIP, SCCP, or H323 traffic. Thus, selecting this option has no effect on devices supporting WMM.

This feature is enabled by default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
svp-prioritization
```

Parameters

None

Example

```
rfs7000-37FABE(config-wlan-qos-test)#svp-prioritization

rfs7000-37FABE(config-wlan-qos-test)#show context
wlan-qos-policy test
 classification non-wmm video
 svp-prioritization
 multicast-mask primary 11-22-33-44-55-66/22-33-44-55-66-77
 classification non-unicast normal
 rate-limit wlan from-air rate 55
 rate-limit wlan from-air max-burst-size 6
 rate-limit wlan from-air red-threshold best-effort 10
 rate-limit client from-air red-threshold background 3
 qos trust dscp
 qos trust wmm
```

```
 accelerated-multicast autodetect classification voice
rfs7000-37FABE(config-wlan-qos-test)#
```

voice-prioritization

wlan-qos-policy

Prioritizes voice clients over other clients (for non-WMM clients). This gives priority to voice and voice management packets and is supported only on certain legacy Brocade VOIP phones. This feature is enabled by default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
voice-prioritization
```

Parameters

None

Example

```
rfs7000-37FABE(config-wlan-qos-test)#voice-prioritization

rfs7000-37FABE(config-wlan-qos-test)#show context
wlan-qos-policy test
 classification non-wmm video
 svp-prioritization
 voice-prioritization
 multicast-mask primary 11-22-33-44-55-66/22-33-44-55-66-77
 classification non-unicast normal
 rate-limit wlan from-air rate 55
 rate-limit wlan from-air max-burst-size 6
 rate-limit wlan from-air red-threshold best-effort 10
 rate-limit client from-air red-threshold background 3
 qos trust dscp
 qos trust wmm
 accelerated-multicast autodetect classification voice
rfs7000-37FABE(config-wlan-qos-test)#
```

wmm

wlan-qos-policy

Configures 802.11e/*Wireless Multimedia* (WMM) parameters for this WLAN QoS policy

WMM makes it possible for both home networks and Enterprises to decide which data streams are most important and assign them a higher traffic priority.

WMM's prioritization capabilities are based on the four access categories (background, best-effort, video, and voice). Higher the *Access Category* (AC) higher is the transmission probability over the controller managed WLAN. ACs correspond to the 802.1d priorities, facilitating interoperability with QoS policy management mechanisms. WMM enabled controllers coexist with legacy devices (not WMM-enabled).

Packets not assigned to a specific access category are categorized as best effort by default. Applications assign each data packet to a given access category. Categorized packets are added to one of four independent transmit queues (one per access category). The client has an internal collision resolution mechanism to address collision among different queues, which selects the frames with the highest priority to transmit.

The same mechanism deals with external collision, to determine which client should be granted the *Opportunity to Transmit* (TXOP). The collision resolution algorithm responsible for traffic prioritization is probabilistic and depends on two timing parameters that vary for each access category. These parameters are:

- The minimum interframe space, or Arbitrary Inter-Frame Space Number (AIFSN)
- The contention window, sometimes referred to as the random back off wait

Both values are smaller for high-priority traffic. The value of the contention window varies through time. Initially the contention window is set to a value that depends on the AC. As frames with the highest AC tend to have the lowest back off values, they are more likely to get a TXOP.

After each collision the contention window is doubled until a maximum value (also dependent on the AC) is reached. After successful transmission, the contention window is reset to its initial, AC dependant value. The AC with the lowest back off value gets the TXOP.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
wmm [background|best-effort|power-save|qbss-load-element|video|voice]

wmm [power-save|qbss-load-element]

wmm [background|best-effort|video|voice] [aifsn <2-15>|cw-max <0-15>|cw-min
<0-15>|
          txop-limit <0-65535>]
```

Parameters

```
wmm [power-save|qbss-load-element]
```

wmm	Configures 802.11e/wireless multimedia parameters
power-save	Enables support for the WMM-Powersave mechanism. This mechanism, also known as *Unscheduled Automatic Power Save Delivery* (U-APSD), is specifically designed for WMM voice devices.
qbss-load-element	Enables support for the *QOS Basic Service Set* (QBSS) load information element in beacons and probe response packets advertised by access packets. This feature is enabled by default.

```
wmm [background|best-effort|video|voice] [aifsn <2-15>|cw-max <0-15>|
cw-min <0-15>|txop-limit <0-65535>]
```

wmm	Configures 802.11e/wireless multimedia parameters. This parameter enables the configuration of four access categories. Applications assign each data packet to one of these four access categories and queues them for transmission.
background	Configures background access category parameters
best-effort	Configures best effort access category parameters. Packets not assigned to any particular access category are categorized by default as having best effort priority
video	Configures video access category parameters
voice	Configures voice access category parameters
aifsn <2-15>	Configures *Arbitrary Inter-Frame Space Number* (AIFSN) from 2 - 15. AIFSN is the wait time between data frames. This parameter is common to background, best effort, video and voice. The default for traffic voice categories is 2 The default for traffic video categories is 2 The default for traffic best effort (normal) categories is 3 The default for traffic background (low) categories is 7 • <2-15> – Sets a value from 2 - 15
cw-max <0-15>	Configures the maximum contention window. Wireless clients pick a number between 0 and the minimum contention window to wait before retransmission. Wireless clients then double their wait time on a collision, until it reaches the maximum contention window. This parameter is common to background, best effort, video and voice. The default for traffic voice categories is 3 The default for traffic video categories is 4 The default for traffic best effort (normal) categories 10 The default for traffic background (low) categories is 10 • <0-15> – ECW: the contention window. The actual value used is (2^ECW - 1). Set a value from 0 - 15.
cw-min <0-15>	Configures the minimum contention window. Wireless clients pick a number between 0 and the min contention window to wait before retransmission. Wireless clients then double their wait time on a collision, until it reaches the maximum contention window. This parameter is common to background, best effort, video and voice. The default for traffic voice categories is 2 The default for traffic video categories is 3 The default for traffic best effort (normal) categories is 4 The default for traffic background (low) categories is 4 • <0-15> – ECW: the contention window. The actual value used is (2^ECW - 1). Set a value from 0 - 15.
txop-limit <0-65535>	Configures the transmit-opportunity (the interval of time during which a particular client has the right to initiate transmissions). This parameter is common to background, best effort, video and voice. The default for traffic voice categories is 47 The default for traffic video categories is 94 The default for traffic best effort (normal) categories is 0 The default for traffic background (low) categories is 0 • <0-65535> – Set a value from 0 - 65535 to configure the transmit-opportunity in 32 microsecond units.

Example

```
rfs7000-37FABE(config-wlan-qos-test)#wmm video txop-limit 9
rfs7000-37FABE(config-wlan-qos-test)#wmm voice cw-min 6

rfs7000-37FABE(config-wlan-qos-test)#show context
wlan-qos-policy test
```

```
 classification non-wmm video
 svp-prioritization
 voice-prioritization
 wmm video txop-limit 9
 wmm voice cw-min 6
 multicast-mask primary 11-22-33-44-55-66/22-33-44-55-66-77
 classification non-unicast normal
 rate-limit wlan from-air rate 55
 rate-limit wlan from-air max-burst-size 6
 rate-limit wlan from-air red-threshold best-effort 10
 rate-limit client from-air red-threshold background 3
 qos trust dscp
 qos trust wmm
 accelerated-multicast autodetect classification voice
rfs7000-37FABE(config-wlan-qos-test)#
```

Chapter

L2TPV3-POLICY

23

This chapter summarizes *Layer 2 Tunnel Protocol Version 3* (L2TPv3) policy commands in the CLI command structure.

The L2TPv3 policy defines control and encapsulation protocols for tunneling different types of layer 2 frames between two IP nodes. The L2TPv3 control protocol controls dynamic creation, maintenance, and tear down of L2TP sessions. The L2TPV3 encapsulation protocol is used to multiplex and de-multiplex L2 data streams between two L2TP nodes across an IP network.

L2TPv3 is an IETF standard used for transporting different types of layer 2 frames in an IP network (and access point profile). L2TPv3 defines control and encapsulation protocols for tunneling layer 2 frames between two IP nodes. Use L2TPv3 to create tunnels for transporting layer 2 frames. L2TPv3 enables Mobility supported controllers and access points to create tunnels for transporting Ethernet frames to and from bridge VLANs and physical ports. L2TPv3 tunnels can be defined between Mobility devices and other vendor devices supporting the L2TPv3 protocol.

Multiple pseudowires can be created within an L2TPv3 tunnel. Mobility supported devices support an Ethernet VLAN pseudowire type exclusively. A pseudowire is an emulation of a layer 2 point-to-point connection over a packet-switching network (PSN). A pseudowire was developed out of the necessity to encapsulate and tunnel layer 2 protocols across a layer 3 network. Ethernet VLAN pseudowires transport Ethernet frames to and from a specified VLAN. One or more L2TPv3 tunnels can be defined between tunnel end points. Each tunnel can have one or more L2TPv3 sessions. Each tunnel session corresponds to one pseudowire. An L2TPv3 control connection (an L2TPv3 tunnel) needs to be established between the tunneling entities before creating a session.

NOTE
A pseudowire is an emulation of a layer 2 point-to-point connection over a *packet-switching network* (PSN). A pseudowire was developed out of the necessity to encapsulate and tunnel layer 2 protocols across a layer 3 network.

Ethernet VLAN pseudowires transport Ethernet frames to and from a specified VLAN. One or more L2TPv3 tunnels can be defined between tunnel end points. Each tunnel can have one or more L2TPv3 sessions. Each tunnel session corresponds to one pseudowire. An L2TPv3 control connection (a L2TPv3 tunnel) needs to be established between the tunneling entities before creating a session.

For optimal pseudowire operation, both the L2TPv3 session originator and responder need to know the psuedowire type and identifier. These two parameters are communicated during L2TPv3 session establishment. An L2TPv3 session created within an L2TPv3 connection also specifies multiplexing parameters for identifying a pseudowire type and ID.

The working status of a pseudowire is reflected by the state of the L2TPv3 session. If a L2TPv3 session is down, the pseudowire associated with it must be shut down. The L2TPv3 control connection keep-alive mechanism can serve as a monitoring mechanism for the pseudowires associated with a control connection.

NOTE
If connecting an Ethernet port to another Ethernet port, the pseudowire type must be *Ethernet port*, if connecting an Ethernet VLAN to another Ethernet VLAN, the pseudowire type must be *Ethernet VLAN*.

This chapter is organized into the following sections:

l2tpv3-policy-commands

L2TPV3-POLICY

Use the (config) instance to configure L2TPv3 policy parameters. To navigate to the L2TPv3 policy instance, use the following commands:

```
<DEVICE>(config)#l2tpv3 policy <L2TPV3-POLICY-NAME>

rfs7000-37FABE(config)#l2tpv3 policy L2TPV3Policy1
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#

rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#?
L2tpv3 Policy Mode commands:
  cookie-size             Size of the cookie field present in each l2tpv3 data
                          message
  failover-delay          Time interval for re-establishing the tunnel after
                          the failover (RF-Domain
                          manager/VRRP-master/Cluster-master failover)
  force-l2-path-recovery  Enables force learning of servers, gateways etc.,
                          behind the l2tpv3 tunnel when the tunnel is
                          established
  hello-interval          Configure the time interval (in seconds) between
                          l2tpv3 Hello keep-alive messages exchanged in l2tpv3
                          control connection
  no                      Negate a command or set its defaults
  reconnect-attempts      Maximum number of attempts to reestablish the
                          tunnel.
  reconnect-interval      Time interval between the successive attempts to
                          reestablish the l2tpv3 tunnel
  retry-attempts          Configure the maximum number of retransmissions for
                          signaling message
  retry-interval          Time interval (in seconds) before the initiating a
                          retransmission of any l2tpv3 signaling message
  rx-window-size          Number of signaling messages that can be received
                          without sending the acknowledgment
  tx-window-size          Number of signaling messages that can be sent
                          without receiving the acknowledgment

  clrscr                  Clears the display screen
  commit                  Commit all changes made in this session
  end                     End current mode and change to EXEC mode
  exit                    End current mode and down to previous mode
  help                    Description of the interactive help system
  revert                  Revert changes
```

```
  service                 Service Commands
  show                    Show running system information
  write                   Write running configuration to memory or terminal

rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#
```

Table 21 summarizes L2TPv3 policy configuration commands.

TABLE 21 L2TPV3-Tunnel-Policy-Config Commands

Command	Description	Reference
cookie-size	Configures the cookie field size for each L2TPv3 data packet	page 1191
failover-delay	Configures the L2TPv3 tunnel failover delay in seconds	page 1192
force-12-path-recovery	Enables the forced detection of servers and gateways behind the L2TPv3 tunnel	page 1193
hello-interval	Configures the interval, in seconds, between L2TPv3 “Hello” keep-alive messages exchanged in the L2TPv3 control connection	page 1194
no	Negates or reverts L2TPv3 tunnel commands	page 1195
reconnect-attempts	Configures the maximum number of retransmissions for signalling messages	page 1196
reconnect-interval	Configures the interval, in seconds, between successive attempts to re-establish a failed tunnel connection	page 1197
retry-attempts	Configures the maximum number of retransmissions of signalling messages	page 1198
retry-interval	Configures the interval, in seconds, before initiating a retransmission of any L2TPv3 signalling message	page 1198
rx-window-size	Configures the number of signalling messages received without sending an acknowledgment	page 1199
tx-window-size	Configures the number of signalling messages transmitted without receiving an acknowledgment	page 1200
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 394
show	Displays running system information	page 429

cookie-size

l2tpv3-policy-commands

Configures the size of the cookie field present in each L2TPv3 data packet. L2TPv3 data packets contain a session cookie that identifies the session (pseudowire) corresponding to it. In a tunnel, the cookie is a 4-byte or 8-byte signature shared between the two tunnel endpoints. This signature is configured at both the source and destination routers. If the signature at both ends do not match, the data is dropped. All sessions within a tunnel have the same session cookie size.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
cookie-size [0|4|8]
```

Parameters

```
cookie-size [0|4|8]
```

cookie-size [0|4|8]	Configures the cookie-field size for each data packet. Select one of the following options: • 0 – No cookie field present in each L2TPv3 data message (this is the default setting) • 4 – 4 byte cookie field present in each L2TPv3 data message • 8 – 8 byte cookie field present in each L2TPv3 data message

Example

```
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#cookie-size 8

rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
 cookie-size 8
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#
```

Related Commands:

no	Resets the cookie-field size to its default (0 - no cookie field present in each L2TPv3 data packet)

failover-delay

l2tpv3-policy-commands

Configures the L2TPv3 tunnel failover delay in seconds. This is the interval after which a failed over tunnel is re-established.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
fail-over <5-60>
```

Parameters

```
fail-over <5-60>
```

fail-over <5-60>	Sets the delay interval to re-establish a failed L2TPv3 tunnel (RF-Domain manager/ VRRP-master/Cluster-master failover) • <5-60> – Specify a failover delay from 5 - 60 seconds. The default is 5 seconds.

Example

```
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#failover-delay 30

rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
 hello-interval 200
 failover-delay 30
 retry-attempts 10
 retry-interval 30
 cookie-size 8
 rx-window-size 9
 tx-window-size 9
 reconnect-interval 100
 reconnect-attempts 8
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#
```

Related Commands:

no	Resets the failover interval to its default (5 seconds)

force-12-path-recovery

l2tpv3-policy-commands

Enables the forced detection of servers and gateways behind the L2TPv3 tunnel. This feature is disabled by default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
force-12-path-recovery
```

Parameters

None

Example

```
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#force-l2-path-recovery

rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
 hello-interval 200
 failover-delay 30
```

```
 retry-attempts 10
 retry-interval 30
 cookie-size 8
 rx-window-size 9
 tx-window-size 9
 reconnect-interval 100
 reconnect-attempts 8
 force-l2-path-recovery
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#
```

Related Commands:

no	Disables the forced detection of servers and gateways behind the L2TPv3 tunnel

hello-interval

l2tpv3-policy-commands

Configures the interval, in seconds, between L2TPv3 “Hello” keep-alive messages exchanged in a L2TPv3 control connection.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
hello-interval <1-3600>
```

Parameters

```
hello-interval <1-3600>
```

hello-interval <1-3600>	Configures the interval for L2TPv3 “Hello” keep-alive messages. Specify a value from 1 - 3600 seconds (default is 60 seconds).

Example

```
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#hello-interval 200

rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
 hello-interval 200
 cookie-size 8
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#
```

Related Commands:

no	Resets the “Hello” keep-alive message interval to its default of 60 seconds

no

l2tpv3-policy-commands

Negates or reverts L2TPv3 policy settings to default

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no [cookie-size|failover-delay|force-12-path-recovery|hello-interval|

reconnect-attempts|reconnect-interval|retry-attempts|retry-interval|rx-window
-size|
          tx-window-size]
```

Parameters

```
no
[cookie-size|failover-delay|force-12-path-recovery|hello-interval|reconnect-a
ttempts|reconnect-interval|retry-attempts|retry-interval|rx-window-size|tx-wi
ndow-size]
```

no cookie-size	Resets the cookie-field size to default (0 - no cookie field present in each L2TPv3 data packet)
no fail-over-delay	Resets the failover interval to its default (5 seconds)
no force-12-path-recovery	Disables the forced detection of servers and gateways behind the L2TPv3 tunnel
no hello-interval	Resets the “Hello” keep-alive message interval to default (60 seconds)
no reconnect-attempts	Resets the maximum number of reconnect attempts to default (0 - configures infinite attempts)
no reconnect-interval	Resets the interval between successive attempts to re-establish a tunnel connection to default (120 seconds)
no retry-attempts	Resets the maximum number of retransmissions for signalling messages to default (5 attempts)
no retry-interval	Resets the interval before initiating a retransmission of a L2TPv3 signalling message to default (5 seconds)
no rx-window-size	Resets the number of packets received without sending an acknowledgment to default (10 packets)
no tx-window-size	Resets the number of packets transmitted without receiving an acknowledgment to default (10 packets)

Example

```
The following example shows the l2tpv3 policy ‘L2TPV3Policy1’ settings before
the ‘no’ commands are executed:

rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
 hello-interval 200
 retry-attempts 10
 retry-interval 30
 cookie-size 8
```

```
 reconnect-interval 100
 reconnect-attempts 50
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#

r(config-l2tpv3-policy-L2TPV3Policy1)#no hello-interval
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#no reconnect-attempts
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#no reconnect-interval
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#no retry-attempts
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#no retry-interval
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#no cookie-size

The following example shows the l2tpv3 policy 'L2TPV3Policy1' settings after
the 'no' commands are executed:

rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#
```

Related Commands:

cookie-size	Configures the cookie-field size present in each L2TPv3 data packet
failover-delay	Configures the L2TPv3 tunnel failover delay in seconds
force-12-path-recovery	Enables the forced detection of servers and gateways behind the L2TPv3 tunnel
hello-interval	Configures the interval for L2TPv3 "Hello" keep-alive messages
reconnect-attempts	Configures the maximum number of attempts made to reestablish a tunnel connection
reconnect-interval	Configures the interval, in seconds, between successive attempts to re-establish a tunnel connection
retry-attempts	Configures the maximum number of retransmissions for signalling messages from 1 - 10
retry-interval	Configures the interval, in seconds, before initiating a retransmission of any L2TPv3 signalling message
rx-window-size	Configures the number of packets received without sending an acknowledgment
tx-window-size	Configures the number of packets transmitted without receiving an acknowledgment

reconnect-attempts

l2tpv3-policy-commands

Configures the maximum number of attempts made to re-establish a tunnel connection

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
reconnect-attempts <0-8>
```

Parameters

```
reconnect-attempts <0-8>
```

reconnect-attempts <0-8>	Configures the maximum number of attempts made to re-establish a tunnel connection from 0 - 8 (default is 0: configures infinite reconnect attempts)

Example

```
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#reconnect-attempts 8

rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
 hello-interval 200
 cookie-size 8
 reconnect-attempts 8
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#
```

Related Commands:

no	Resets the maximum number of reconnect attempts to default (0: configures infinite reconnect attempts)

reconnect-interval

l2tpv3-policy-commands

Configures the interval, in seconds, between two successive attempts to re-establish a failed tunnel connection

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
reconnect-interval <1-3600>
```

Parameters

```
reconnect-interval <1-3600>
```

reconnect-interval <1-3600>	Configures the interval between successive attempts to re-establish a failed tunnel connection. Specify a value from 1 - 3600 seconds (default is 120 seconds).

Example

```
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#reconnect-interval 100

l2tpv3 policy L2TPV3Policy1
 hello-interval 200
 cookie-size 8
 reconnect-interval 100
 reconnect-attempts 8
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#
```

Related Commands:

no	Resets the interval between successive attempts to re-establish a failed tunnel connection to default (120 seconds)

retry-attempts

l2tpv3-policy-commands

Configures the maximum number of attempts made to retransmit signalling messages. Use this command to specify how many retransmission cycles occur before determining the target tunnel peer is not reachable.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
retry-attempts <1-10>
```

Parameters

```
retry-attempts <1-10>
```

retry-attempts <1-10>	Configures the maximum number of attempts made to retransmit signalling messages from 1 - 10 (default is 5 attempts)

Example

```
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#retry-attempts 10

rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
 hello-interval 200
 retry-attempts 10
 cookie-size 8
 reconnect-interval 100
 reconnect-attempts 8
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#
```

Related Commands:

no	Resets the maximum number of retransmissions of signalling messages to default (5 attempts)

retry-interval

l2tpv3-policy-commands

Configures the interval, in seconds, between two successive attempts at retransmitting a L2TPv3 signalling message

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
retry-interval <1-250>
```

Parameters

```
retry-interval <1-250>
```

retry-interval <1-250>	Configures the interval, in seconds, between two successive retransmission attempts. Specify a value from 1 - 250 seconds (default is 5 seconds).

Example

```
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#retry-interval 30

rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
 hello-interval 200
 retry-attempts 10
 retry-interval 30
 cookie-size 8
 reconnect-interval 100
 reconnect-attempts 8
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#
```

Related Commands:

no	Resets the retry interval to default (5 seconds)

rx-window-size

l2tpv3-policy-commands

Configures the number of signalling packets received without sending an acknowledgment

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
rx-window-size <1-15>
```

Parameters

```
rx-window-size <1-15>
```

rx-window-size <1-15>	Configures the number of packets received without sending an acknowledgment. Specify a value from 1 - 15 (default is 10 packets).

Example

```
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#rx-window-size 9

rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
 hello-interval 200
 retry-attempts 10
 retry-interval 30
 cookie-size 8
 rx-window-size 9
 reconnect-interval 100
 reconnect-attempts 8
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#
```

Related Commands:

no	Resets the number of packets received without sending an acknowledgment to default (10 packets)

tx-window-size

l2tpv3-policy-commands

Configures the number of signalling packets transmitted without receiving an acknowledgment

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
tx-window-size <1-15>
```

Parameters

```
tx-window-size <1-15>
```

tx-window-size <1-15>	Configures the number of packets transmitted without receiving an acknowledgment. Specify a value from 1 - 15 (default is 10 packets).

Example

```
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#tx-window-size 9

rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#show context
```

```
l2tpv3 policy L2TPV3Policy1
 hello-interval 200
 retry-attempts 10
 retry-interval 30
 cookie-size 8
 rx-window-size 9
 tx-window-size 9
 reconnect-interval 100
 reconnect-attempts 8
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#
```

Related Commands:

no	Resets the number of packets transmitted without receiving an acknowledgment to default (10 packets)

l2tpv3-tunnel-commands

L2TPV3-POLICY

Use the (profile or device context) instance to configure a L2TPv3 tunnel. To navigate to the tunnel configuration mode, use the following command in the profile context:

```
<DEVICE>(config-profile-default-rfs7000)#l2tpv3 tunnel <TUNNEL-NAME>

rfs7000-37FABE(config-profile-default-rfs7000)#l2tpv3 tunnel Tunnel1
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#

rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#?
L2tpv3 Tunnel Mode commands:
  L2tpv3 Tunnel Mode commands:
  establishment-criteria  Set tunnel establishment criteria
  hostname                Tunnel specific local hostname
  local-ip-address        Configure the IP address for tunnel. If not
                          specified, tunnel source ip address would be chosen
                          automatically based on the tunnel peer ip address
  mtu                     Configure the mtu size for the tunnel
  no                      Negate a command or set its defaults
  peer                    Configure the l2tpv3 tunnel peers. At least one peer
                          must be specified
  router-id               Tunnel specific local router ID
  session                 Create / modify the specified l2tpv3 session
  use                     Set setting to use

  clrscr                  Clears the display screen
  commit                  Commit all changes made in this session
  end                     End current mode and change to EXEC mode
  exit                    End current mode and down to previous mode
  help                    Description of the interactive help system
  revert                  Revert changes
  service                 Service Commands
  show                    Show running system information
  write                   Write running configuration to memory or terminal

rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#
```

The following table summarizes L2TPv3 tunnel configuration commands.

Command	Description	Reference
establishment-criteria	Configures L2TPv3 tunnel establishment criteria	page 1202
hostname	Configures tunnel specific local hostname	page 1203
local-ip-address	Configures the tunnel's IP address	page 1204
mtu	Configures the tunnel's *Maximum Transmission Unit* (MTU) size	page 1205
no	Negates or reverts L2TPv3 tunnel commands	page 1205
peer	Configures the tunnel's peers	page 1207
router-id	Configures the tunnel's local router ID	page 1209
session	Creates/modifies specified L2TPv3 session	page 1210
use	Configures a tunnel to use a specified L2TPv3 tunnel policy	page 1211
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

establishment-criteria

l2tpv3-tunnel-commands

Configures L2TPv3 tunnel establishment criteria

A L2TPv3 tunnel is established from the current device to the NOC controller when the current device becomes the VRRP master, cluster master, or RF Domain manager. Similarly, the L2TPv3 tunnel is closed when the current device switches to standby or backup mode.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
establishment-criteria [always|cluster-master|rf-domain-manager|vrrp-master
<1-255>]
```

Parameters

```
establishment-criteria [always|cluster-master|rf-domain-manager|vrrp-master
<1-255>]
```

always	Always establishes a L2TPv3 tunnel from the current device to the NOC controller. This is the default setting.
cluster-master	Establishes a L2TPv3 tunnel from the current device to the NOC controller, only when the current device becomes the cluster master **NOTE:** The L2TPv3 tunnel is closed when the current device switches back the standby or backup mode.
rf-domain-manager	Establishes a L2TPv3 tunnel from the current device to the NOC controller, only when the current device becomes the RF Domain manager **NOTE:** The L2TPv3 tunnel is closed when the current device switches back the standby or backup mode.
vrrp-master <1-255>	Establishes a L2TPv3 tunnel from the current device to the NOC controller, only when the current device becomes the VRRP master • <1-255> – Specify the VRRP group number from 1 - 255. **NOTE:** The L2TPv3 tunnel is closed when the current device switches back the standby or backup mode.

Example

```
rfs7000-37FABE(config-profile
default-rfs7000-l2tpv3-tunnel-Tunnel1)#establishment-criteria cluster-master

rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#show
context
 l2tpv3 tunnel Tunnel1
  establishment-criteria cluster-master
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#
```

Related Commands:

no	Resets to default (always)

hostname

l2tpv3-tunnel-commands

Configures the tunnel's local hostname

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
hostname <WORD>
```

Parameters

```
hostname <WORD>
```

hostname <WORD>	Configures the tunnel's local hostname • <WORD> – Specify the tunnel's local hostname.

Example

```
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#hostname
TunnelHost1

rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#show
context
 l2tpv3 tunnel Tunnel1
  hostname TunnelHost1
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#
```

Related Commands:

no	Removes the tunnel's local hostname

local-ip-address

l2tpv3-tunnel-commands

Configures the tunnel's source IP address. If no IP address is specified, the tunnel's source IP address is automatically configured based on the tunnel's peer IP address.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
local-ip-address <IP>
```

Parameters

```
local-ip-address <IP>
```

local-ip-address <IP>	Configures the L2TPv3 tunnel's source IP address • <IP> – Specify the tunnel's IP address. Ensure the IP address is available (or will become available - virtual IP) on an interface. Modifying a tunnel's local IP address re-establishes the tunnel.

Example

```
rfs7000-37FABE(config-profile
default-rfs7000-l2tpv3-tunnel-Tunnel1)#local-ip-address 172.16.10.2

rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#show
context
 l2tpv3 tunnel Tunnel1
  local-ip-address 172.16.10.2
  hostname TunnelHost1
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#
```

Related Commands:

no	Resets the tunnel's local IP address and re-establishes the tunnel

mtu

l2tpv3-tunnel-commands

Configures the *Maximum Transmission Unit* (MTU) size for this tunnel. This value determines the packet size transmitted over this tunnel.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
mtu <128-1460>
```

Parameters

```
mtu <128-1460>
```

mtu <128-1460>	Configures the MTU size for this tunnel. Specify a value from 128 - 1460 bytes (default is 1460 bytes).

Example

```
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#mtu 1280

rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#show
context
 l2tpv3 tunnel Tunnel1
  local-ip-address 172.16.10.2
  mtu 1280
  hostname TunnelHost1
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#
```

Related Commands:

no	Resets the MTU size for this tunnel to default (1460 bytes)

no

l2tpv3-tunnel-commands

Negates or reverts a L2TPv3 tunnel settings to default

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no
[establishment-criteria|hostname|local-ip-address|mtu|peer|router-id|session|
use]
```

Parameters

```
no
[establishment-criteria|hostname|local-ip-address|mtu|peer|router-id|session|
use]
```

establishment-criteria	Resets the tunnel's establishment criteria to default
no hostname	Removes the tunnel's local hostname
no local-ip-address	Resets the tunnel's local IP address and re-establishes the tunnel
no mtu	Resets the MTU size for this tunnel to default (1460 bytes)
no peer	Removes the peer configured for this tunnel
no router-id	Removes the tunnel's router ID
no session	Removes a session
no use	Removes the L2TPv3 policy associated with a tunnel and reverts to the default tunnel policy

Example

```
The tunnel settings before the 'no' command is executed:

rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#show
context
 l2tpv3 tunnel Tunnel1
  local-ip-address 172.16.10.2
  mtu 1280
  hostname TunnelHost1
  establishment-criteria cluster-master
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#

The tunnel settings after the 'no' command is executed:

rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#no
local-ip
-address
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#no mtu
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#no
hostname

rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#show
context
 l2tpv3 tunnel Tunnel1
  establishment-criteria cluster-master
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#
```

Related Commands:

establishment-criteria	Configures a L2TPv3 tunnel's establishment criteria
hostname	Configures the tunnel's local hostname
local-ip-address	Configures the tunnel's source IP address
mtu	Configures the MTU size for this tunnel
peer	Configures the tunnel's peers
router-id	Configures the tunnel's local router ID
session	Creates/modifies specified L2TPv3 session
use	Associates a specified L2TPv3 tunnel policy with a L2TPv3 tunnel

peer

l2tpv3-tunnel-commands

Configures the L2TPv3 tunnel's peers. At least one peer must be specified.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
peer <1-2> {hostname|ip-address|ipsec-secure|router-id|udp}

peer <1-2> {hostname [<HOSTNAME>|any]} {ipsec-secure|router-id|udp}
peer <1-2> {ip-address <IP>} {hostname|ipsec-secure|router-id|udp}
peer <1-2> {ipsec-secure} {gw [<IP>|<WORD>]}
peer <1-2> {router-id [<IP>|<WORD>|any]} {ipsec-secure|udp}
peer <1-2> {udp} {ipsec-secure|port <1-65535>}
```

Parameters

```
peer <1-2> {hostname [<HOSTNAME>|any]} {ipsec-secure|router-id|udp}
```

peer <1-2>	Configures the tunnel's peer ID from 1 - 2 **NOTE:** At any time the tunnel is established with only one peer.
hostname [<HOSTNAME>|any]	Optional. Configures the peers' hostname. The hostname options are: • <HOSTNAME> – Specifies the hostname as *Fully Qualified Domain Name* (FQDN) or partial DN or any other name • any – Peer name is not specified. If the hostname is 'any' this tunnel is considered as responder only and will allow incoming connection from any host.
ipsec-secure {gw [<IP>|<WORD>]}	After specifying the peer hostname, optionally specify the IPSec settings: • ipsec-secure – Optional. Enables auto IPSec • gw – Optional. Configures IPSec gateway IP address or hostname • <IP> – Configures IPSec gateway's IP address • <WORD> – Configures IPSec gateway's hostname

router-id [<IP>|<WORD>|any]	After specifying the peer hostname, optionally specify router ID settings: • router-id – Optional. Configures the peer's router ID in one of the following formats: • <IP> – Peer router ID in the IP address (A.B.C.D) format • <WORD> – Peer router ID range (for example, 100-120) • any – Peer router ID is not specified. This allows incoming connection from any router ID.
udp {ipsec-secure gw| port <1-65535> {ipsec-secure}}	After specifying the peer hostname, optionally specify UDP settings: The UDP option configures the encapsulation mode for this tunnel. • UDP – Optional. Configures UDP encapsulation (default encapsulation is IP) • ipsec-secure gw – Optional. Enables auto IPSec • port <1-65535> {ipsec-secure} – Optional. Configures the peer's UDP port running the L2TPv3 service from 1 - 65535. After specifying the peer UDP port, optionally configure the IPSec settings.

`peer <1-2> {ip-address <IP>} {hostname|ipsec-secure|router-id|udp}`

peer <1-2>	Configures the tunnel's peer ID from 1 - 2. At any time the tunnel is established with only one peer.
ip-address <IP>	Optional. Configures the peer's IP address in the A.B.C.D format
hostname [<FQDN>|any]	After specifying the peer IP address, optionally specify the peer's hostname: Optional. Configures the peers' hostname. The hostname options are: • <FQDN> – Specifies the hostname as FQDN or partial DN • any – Peer name is not specified. If the hostname is 'any' this tunnel is considered as responder only and will allow incoming connection from any host.
ipsec-secure {gw [<IP>|<WORD>]}	After specifying the peer IP address, optionally specify the IPSec settings: • ipsec-secure – Optional. Enables auto IPSec • gw – Optional. Configures IPSec gateway IP address or hostname • <IP> – Configures IPSec gateway's IP address • <WORD> – Configures IPSec gateway's hostname
router-id [<A.B.C.D>|<WORD>|any]	After specifying the peer IP address, optionally specify the router ID using one of the following options: • router-id – Optional. Configures the peer's router-id in one of the following formats: • <A.B.C.D> – Peer router ID in the IP address (A.B.C.D) format • <WORD> – Peer router ID range (for example, 100-120) • any – Peer router ID is not specified. This allows incoming connection from any router ID.
udp {ipsec-secure gw| port <1-65535> {ipsec-secure}}	After specifying the peer IP address, optionally specify the peer's UDP port settings: The UDP option configures the encapsulation mode for this tunnel. • UDP – Optional. Configures UDP encapsulation (default encapsulation is IP) • ipsec-secure gw – Optional. Enables auto IPSec • port <1-65535> – Optional. Configures the peer's UDP port running the L2TPv3 service from 1 - 65535. After specifying the peer UDP port, optionally configure the IPSec settings.

`peer <1-2> {ipsec-secure} {gw [<IP>|<WORD>]}`

peer <1-2>	Configures the tunnel's peer ID from 1 - 2. At any time the tunnel is established with only one peer.
ipsec-secure {gw [<IP>|<WORD>]}	Optional. Enables auto IPSec for this peer • gw – Optional. Configures IPSec gateway IP address or hostname • <IP> – Configures IPSec gateway's IP address • <WORD> – Configures IPSec gateway's hostname

`peer <1-2> {router-id [<IP>|<WORD>|any]} {ipsec-secure|udp}`

peer <1-2>	Configures the tunnel peer ID from 1 - 2. At any time the tunnel is established with only one peer.
router-id [<A.B.C.D>|<WORD>|any]	Optional. Configures the peer's router-id in one of the following formats: • <A.B.C.D> – Peer router ID in the IP address (A.B.C.D) format • <WORD> – Peer router ID range (for example, 100-120) any – Peer router ID is not specified. This allows incoming connection from any router ID.
ipsec-secure {gw [<IP>|<WORD>]}	After specifying the peer's router ID, optionally specify the IPSec settings. • ipsec-secure – Optional. Enables auto IPSec • gw – Optional. Configures IPSec gateway IP address or hostname • <IP> – Configures IPSec gateway's IP address • <WORD> – Configures IPSec gateway's hostname
udp {ipsec-secure gw| port <1-65535> {ipsec-secure}}	After specifying the peer's router ID, optionally specify the IPSec settings. The UDP option configures the encapsulation mode for this tunnel. • UDP – Optional. Configures UDP encapsulation (default encapsulation is IP) • ipsec-secure gw – Optional. Enables auto IPSec • port <1-65535> – Optional. Configures the peer's UDP port running the L2TPv3 service from 1 - 65535. After specifying the peer UDP port, optionally configure the IPSec settings.

`peer <1-2> {udp} {ipsec-secure|port <1-65535>}`

peer <1-2>	Configures the tunnel peer ID from 1 - 2. At any time the tunnel is established with only one peer.
udp {ipsec-secure| port <1-65535> {ipsec-secure}}	Optional. Configures UDP encapsulation for this tunnel's pee (default encapsulation is IP) • ipsec-secure – Optional. Configures IPSec gateway on this peer UDP port • port <1-65535> – Optional. Configures the peer's UDP port running the L2TPv3 service from 1 - 65535. After specifying the peer UDP port, optionally configure the IPSec settings.

Example

```
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#peer 2
hostname tunnel1peer1 udp port 100

rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#show
context
 l2tpv3 tunnel Tunnel1
  peer 2 hostname tunnel1peer1 udp port 100
  establishment-criteria cluster-master
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#
```

Related Commands:

no	Removes the peer configured for this tunnel

router-id

l2tpv3-tunnel-commands

Configures the tunnel's local router ID

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
router-id [<1-4294967295>|<IP>]
```

Parameters

```
router-id [<1-4294967295>|<IP>]
```

router-id [<1-4294967295>|<IP>]	Configures the tunnel's local router ID in one of the following formats: • <1-4294967295> – Router ID in the number format (from1- 4294967295) • <IP> – Router ID in IP address format (A.B.C.D)

Example

```
rfs7000-37FABE(config-profile
default-rfs7000-l2tpv3-tunnel-Tunnel1)#router-id 2000

rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#show
context
 l2tpv3 tunnel Tunnel1
  peer 2 hostname tunnel1peer1 udp port 100
  router-id 2000
  establishment-criteria cluster-master
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#
```

Related Commands:

no	Removes the tunnel's router ID

session

l2tpv3-tunnel-commands

Configures a session's pseudowire ID, which describes the session's purpose. The session established message sends this pseudowire ID to the L2TPv3 peer.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
session <L2TPV3-SESSION-NAME> pseudowire-id <1-4294967295> traffic-source
          vlan <VLAN-ID-RANGE> {native-vlan <1-4094>}
```

Parameters

```
session <L2TPV3-SESSION-NAME> pseudowire-id <1-4294967295> traffic-source
       vlan <VLAN-ID-RANGE> {native-vlan <1-4094>}
```

session <L2TPV3-SESSION-NAME>	Configures this session's name
pseudowire-id <1-4294967295>	Configures the pseudowire ID for this session from 1- 4204067295
traffic-source vlan <VLAN-ID-RANGE>	Configures VLAN as the traffic source for this tunnel • <VLAN-ID-RANGE> – Configures VLAN range list of traffic source. Specify the VLAN IDs as a range (for example, 10-20, 25, 30-35).
native-vlan <1-4094>	Optional – Configures the native VLAN ID for this session, which is not tagged • <1-4094> – Specify the native VLAN ID from 1- 4094.

Usage Guidelines:

The working status of a pseudowire is reflected by the state of the L2TPv3 session. If the corresponding session is L2TPv3 down, the pseudowire associated with it must be shut down.

Example

```
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#session
tunnel1peer1session1 pseudowire-id 5000 traffic-source vlan 10-20 native-vlan
1

rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#show
context
 l2tpv3 tunnel Tunnel1
  peer 2 hostname tunnel1peer1 udp port 100
  session tunnel1peer1session1 pseudowire-id 5000 traffic-source vlan 10-20
native-vlan 1
  router-id 2000
  establishment-criteria cluster-master
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#
```

Related Commands:

no	Removes a session

use

l2tpv3-tunnel-commands

Configures a tunnel to use a specified L2TPv3 tunnel policy and specified critical resources

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
use [critical-resource|l2tpv3-policy]
```

```
use critical-resource <CRM-NAME1> {<CRM-NAME2>} <CRM-NAME3>} <CRM-NAME4>}
use l2tpv3-policy <L2TPV3-POLICY-NAME>
```

Parameters

```
use critical-resource <CRM-NAME1> {<CRM-NAME2>} {<CRM-NAME3>} {<CRM-NAME4>}
```

use critical-resource <CRM-NAME1> {<CRM-NAME2>} {<CRM-NAME3>} {<CRM-NAME4>}	Specifies the critical resource(s) to use with this tunnel • <CRM1-NAME> – Specify the first critical resource name • <CRM-NAME2/3/4> – Optional. Specify the second/third/fourth critical resource names. Maximum of four critical resources can be monitored. **NOTE:** In case of tunnel initiator, L2TPv3 tunnel is established only if the critical resources identified by the <CRM-NAME1>..... <CRM-NAME4> arguments are available at the time of tunnel establishment. **NOTE:** In case of L2TPv3 tunnel termination, all incoming tunnel establishment requests are rejected if the critical resources specified by the <CRM-NAME1>..... <CRM-NAME4> arguments are not available.

```
use l2tpv3-policy <L2TPV3-POLICY-NAME>
```

use l2tpv3-policy <L2TPV3-POLICY-NAME>	Associates a specified L2TPv3 policy with this tunnel • <L2TPV3-POLICY-NAME> – Specify the policy name.

Example

```
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#use
l2tpv3-
policy L2TPV3Policy1

rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#show
context
 l2tpv3 tunnel Tunnel1
  peer 2 hostname tunnel1peer1 udp port 100
  use l2tpv3-policy L2TPV3Policy1
  session tunnel1peer1session1 pseudowire-id 5000 traffic-source vlan 10-20
native-vlan 1
  router-id 2000
  establishment-criteria cluster-master
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#
```

Related Commands:

no	Removes the L2TPv3 policy configured with a tunnel and reverts to the default tunnel policy

l2tpv3-manual-session-commands

L2TPV3-POLICY

After a successful tunnel connection and establishment, individual sessions can be created. Each session is a single data stream. After successful session establishment, data corresponding to that session (pseudowire) can be transferred. If a session is down, the pseudowire associated with it is shut down as well.

Use the (profile-context) instance to manually configure a L2TPv3 session. To navigate to the L2TPv3 manual session configuration mode, use the following command in the profile context:

```
<DEVICE>(config-profile-default-rfs7000)#l2tpv3 manual-session <SESSION-NAME>
```

```
rfs7000-37FABE(config-profile-default-rfs7000)#l2tpv3 manual-session test
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#

rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#?
L2tpv3 Manual Session Mode commands:
  local-cookie       The local cookie for the session
  local-ip-address   Configure the IP address for tunnel. If not specified,
                     tunnel source ip address would be chosen automatically
                     based on the tunnel peer ip address
  local-session-id   Local session id for the session
  mtu                Configure the mtu size for the tunnel
  no                 Negate a command or set its defaults
  peer               Configure L2TPv3 manual session peer
  remote-cookie      The remote cookie for the session
  remote-session-id  Remote session id for the session
  traffic-source     Traffic that is tunneled

  clrscr             Clears the display screen
  commit             Commit all changes made in this session
  end                End current mode and change to EXEC mode
  exit               End current mode and down to previous mode
  help               Description of the interactive help system
  revert             Revert changes
  service            Service Commands
  show               Show running system information
  write              Write running configuration to memory or terminal

rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#
```

The following table summarizes L2TPv3 manual session configuration commands.

Command	Description	Reference
local-cookie	Configures the manual session's local cookie field size	page 1214
local-ip-address	Configures the manual session's local source IP address	page 1214
local-session-id	Configures the manual session's local session ID	page 1215
mtu	Configures the MTU size for the manual session tunnel	page 1216
no	Negates or reverts L2TPv3 manual session commands to default	page 1205
peer	Configures the manual session's peers	page 1218
remote-cookie	Configures the remote cookie for the manual session	page 1219
remote-session-id	Configures the manual session's remote session ID	page 1220
traffic-source	Configures the traffic source tunneled by the manual session	page 1221
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 394

Command	Description	Reference
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

local-cookie

l2tpv3-manual-session-commands

Configures the local cookie field size for the manual session

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
local-cookie size [4|8] <1-4294967295> {<1-4294967295>}
```

Parameters

```
local-cookie size [4|8] <1-4294967295> {<1-4294967295>}
```

local-cookie size [4|8]	Configures the local cookie field size for this manual session. The options are: • 4 – 4 byte local cookie field • 8 – 8 byte local cookie field
<1-4294967295>	Configures the local cookie value first word. Applies to both the 4 byte and 8 byte local cookies
<1-4294967295>	Optional – Configures the local cookie value second word. Applicable to only 8 byte cookies. This parameter is ignored for 4 byte cookies.

Example

```
rfs7000-37FABE(config-profile
default-rfs7000-l2tpv3-manual-session-test)#local-cookie size 8 200 300

rfs7000-37FABE(config-profile
default-rfs7000-l2tpv3-manual-session-test)#show context
 l2tpv3 manual-session test
  local-cookie size 8 200 300
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#
```

Related Commands:

no	Removes the local cookie size configured for a manual session

local-ip-address

l2tpv3-manual-session-commands

Configures the manual session's source IP address. If no IP address is specified, the tunnel's source IP address is automatically configured based on the tunnel peer IP address. This parameter is applicable when establishing the session and responding to incoming requests.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
local-ip-address <IP>
```

Parameters

```
local-ip-address <IP>
```

local-ip-address <IP>	Configures the manual session's source IP address in the A.B.C.D format

Example

```
rfs7000-37FABE(config-profile
default-rfs7000-l2tpv3-manual-session-test#local-ip-address 1.2.3.4

rfs7000-37FABE(config-profile
default-rfs7000-l2tpv3-manual-session-test)#show context
 l2tpv3 manual-session test
 local-cookie size 8 200 300
 local-ip-address 1.2.3.4
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#
```

Related Commands:

no	Resets the manual session's local source IP address. This re-establishes the session.

local-session-id

l2tpv3-manual-session-commands

Configures the manual session's local session ID

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
local-session-id <1-63>
```

Parameters

```
local-session-id <1-63>
```

local-session-id <1-63>	Configures this manual session's local session ID from 1 - 63. This is the pseudowire ID for the session. This pseudowire ID is sent in a session establishment message to the L2TP peer.

Example

```
rfs7000-37FABE(config-profile
default-rfs7000-l2tpv3-manual-session-test)#local-session-id 1

rfs7000-37FABE(config-profile
default-rfs7000-l2tpv3-manual-session-test)#show context
 l2tpv3 manual-session test
  local-cookie size 8 200 300
  local-ip-address 1.2.3.4
  local-session-id 1
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#
```

Related Commands:

no	Removes the manual session's local session ID

mtu

l2tpv3-manual-session-commands

Configures the *Maximum Transmission Unit* (MTU) size for the manual session tunnel. The MTU is the size (in bytes) of the largest protocol data unit the layer can pass between tunnel peers in this session. A larger MTU means processing fewer packets for the same amount of data.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
mtu <128-1460>
```

Parameters

```
mtu <128-1460>
```

mtu <128-1460>	Configures the MTU size for this manual session tunnel. Specify a value from 128 - 1460 bytes (default is 1460 bytes).

Example

```
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#mtu
200

rfs7000-37FABE(config-profile
default-rfs7000-l2tpv3-manual-session-test)#show context
```

```
 l2tpv3 manual-session test
  local-cookie size 8 200 300
  local-ip-address 1.2.3.4
  mtu 200
  local-session-id 1
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#
```

Related Commands:

no	Resets the MTU size for this manual session to default (1460 bytes)

no

l2tpv3-manual-session-commands

Negates or reverts L2TPv3 manual session settings to default

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no [local-cookie|local-ip-address|local-session-id|mtu|peer|remote-cookie|
          remote-session-id|traffic-source]
```

Parameters

```
no [local-cookie|local-ip-address|local-session-id|mtu|peer|remote-cookie|
remote-session-id|traffic-source]
```

no local-cookie	Removes the local cookie size configured for a manual session
no local-ip-address	Resets the manual session's local source IP address and re-establishes the tunnel
no local-session-id	Removes the manual session's local session ID
no mtu	Resets the manual session's MTU size to default (1460 bytes)
no peer	Removes the peer configuration from this tunnel
no remote-cookie	Removes the remote cookie field size
no remote-session-id	Removes the manual session's remote session ID
no traffic-source	Removes the configured traffic source

Example

```
The following example shows the manual session 'test' settings before the 'no'
commands are executed:

rfs7000-37FABE(config-profile
default-rfs7000-l2tpv3-manual-session-test)#show context
 l2tpv3 manual-session test
  local-ip-address 1.2.3.4
```

```
  peer ip-address 5.6.7.8 udp port 150
  traffic-source vlan 50-60 native-vlan 2
  local-session-id 1
  remote-session-id 200
  remote-cookie size 8 400 700
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#

rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#no
local-ip-address
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#no
local-session-id
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#no
remote-session-id

The following example shows the manual session 'test' settings after the 'no'
commands are executed:

rfs7000-37FABE(config-profile
default-rfs7000-l2tpv3-manual-session-test)#show context
 l2tpv3 manual-session test
  peer ip-address 5.6.7.8 udp port 150
  traffic-source vlan 50-60 native-vlan 2
  remote-cookie size 8 400 700
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#
```

Related Commands:

local-cookie	Configures the local cookie field size for the manual session
local-ip-address	Configures the manual session's local source IP address
local-session-id	Removes the manual session's local session ID
mtu	Configures the manual session's MTU size
peer	Configures the manual session's peers
remote-cookie	Configures the manual session's remote cookie field size
remote-session-id	Configures the manual session's remote session ID
traffic-source	Configures the traffic source tunneled in this session

peer

l2tpv3-manual-session-commands

Configures peer(s) allowed to establish the manual session tunnel. The peers are identified by their IP addresses.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
peer ip-address <IP> {udp {port <1-65535>}}
```

Parameters

```
peer ip-address <IP> {udp {port <1-65535>}}
```

peer ip-address <IP>	Configures the tunnel's peer IP address in the A.B.C.D format
udp {port <1-65335>}	Optional. Configures the UDP encapsulation mode for this tunnel (default encapsulation is IP) • port <1-65535> – Optional. Configures the peer's UDP port running the L2TPv3 service. Specify a value from 1 - 65535.

Example

```
rfs7000-37FABE(config-profile
default-rfs7000-l2tpv3-manual-session-test)#peer
ip-address 5.6.7.8 udp port 150

rfs7000-37FABE(config-profile
default-rfs7000-l2tpv3-manual-session-test)#show context
 l2tpv3 manual-session test
  local-cookie size 8 200 300
  local-ip-address 1.2.3.4
  peer ip-address 5.6.7.8 udp port 150
  mtu 200
  local-session-id 1
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#
```

Related Commands:

no	Removes the manual session's peer

remote-cookie

l2tpv3-manual-session-commands

Configures the manual session's remote cookie field size

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
remote-cookie size [4|8] <1-4294967295> {<1-4294967295>}
```

Parameters

```
remote-cookie size [4|8] <1-4294967295> {<1-4294967295>}
```

remote-cookie size [4|8]	Configures the remote cookie field size for this manual session. The options are: • 4 – 4 byte remote cookie field • 8 – 8 byte remote cookie field
<1-4294967295>	Configures the remote cookie value first word. Applies to both the 4 byte and 8 byte local cookies
<1-4294967295>	Optional – Configures the remote cookie value second word. Applicable to only 8 byte cookies. This parameter is ignored for 4 byte cookies.

Example

```
rfs7000-37FABE(config-profile
default-rfs7000-l2tpv3-manual-session-test)#remote-cookie size 8 400 700

rfs7000-37FABE(config-profile
default-rfs7000-l2tpv3-manual-session-test)#show context
 l2tpv3 manual-session test
  local-ip-address 1.2.3.4
  peer ip-address 5.6.7.8 udp port 150
  mtu 200
  local-session-id 1
  remote-cookie size 8 400 700
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#
```

Related Commands:

no	Removes the manual session's remote cookie field size

remote-session-id

l2tpv3-manual-session-commands

Configures the manual session's remote ID. This ID is passed in the establishment of the tunnel session.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
remote-session-id <1-4294967295>
```

Parameters

```
remote-session-id <1-4294967295>
```

remote-session-id <1-4294967295>	Configures this manual session's remote ID. Specify a value from 1 - 4294967295.

Example

```
rfs7000-37FABE(config-profile
default-rfs7000-l2tpv3-manual-session-test)#remote-session-id 200

rfs7000-37FABE(config-profile
default-rfs7000-l2tpv3-manual-session-test)#show context
 l2tpv3 manual-session test
  local-ip-address 1.2.3.4
  peer ip-address 5.6.7.8 udp port 150
  local-session-id 1
  remote-session-id 200
  remote-cookie size 8 400 700
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#
```

Related Commands:

no	Removes the manual session's remote ID

traffic-source

l2tpv3-manual-session-commands

Configures the traffic source tunneled by this session

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
traffic-source vlan <VLAN-ID-RANGE> {native-vlan <1-4094>}
```

Parameters

```
traffic-source vlan <VLAN-ID-RANGE> {native-vlan <1-4094>}
```

traffic-source vlan <VLAN-ID-RANGE>	Configures VLAN as the traffic source for this tunnel • <VLAN-ID-RANGE> – Configures VLAN range list of traffic source. Specify the VLAN IDs as a range (for example, 10-20, 25, 30-35)
native-vlan <1-4094>	Optional – Configures the native VLAN ID for this session, which is not tagged • <1-4094> – Specify the native VLAN ID from 1- 4094.

Example

```
rfs7000-37FABE(config-profile
default-rfs7000-l2tpv3-manual-session-test)#traffic-source vlan 50-60
native-vlan 2

rfs7000-37FABE(config-profile
default-rfs7000-l2tpv3-manual-session-test)#show context
 l2tpv3 manual-session test
  local-ip-address 1.2.3.4
```

```
    peer ip-address 5.6.7.8 udp port 150
    traffic-source vlan 50-60 native-vlan 2
    local-session-id 1
    remote-session-id 200
    remote-cookie size 8 400 700
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#
```

Related Commands:

no	Removes the traffic source configured for a tunnel

Chapter

ROUTER-MODE COMMANDS

24

This chapter summarizes *Open Shortest Path First* (OSPF) router mode commands in the CLI command structure. All router-mode commands are available on both device and profile modes.

OSPF is an *interior gateway protocol* (IGP) used within large autonomous systems to distribute routing information. OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighbor routers and constructs a network topology. The topology determines the routing table presented to the Internet Layer, which makes routing decisions based solely on the destination IP address found in IP packets.

OSPF detects changes in the topology, like a link failure, and plots a new loop-free routing structure. It computes the shortest path for each route using a shortest path first algorithm. Link state data is maintained on each router and is periodically updated on all OSPF member routers. This enables routers to synchronize routing tables.

OSPF uses a route table managed by the link cost (external metrics) defined for each routing interface. The cost could be the distance of a router (round-trip time), link throughput or link availability.

Use the (config) instance to configure router commands. To navigate to the (config-router-mode) instance, use the following command:

```
<DEVICE>(config-profile-<PROFILE-NAME>)#router ospf
<DEVICE>(config-profile <PROFILE-NAME>-router-ospf)#

rfs7000-37FABE(config-profile-default-rfs7000)#router ospf
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#

rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#?
Router OSPF Mode commands:
  area                  OSPF area
  auto-cost             OSPF auto-cost
  default-information   Distribution of default information
  ip                    Internet Protocol (IP)
  network               OSPF network
  no                    Negate a command or set its defaults
  ospf                  OSPF
  passive               Make OSPF Interface as passive
  redistribute          Route types redistributed by OSPF
  route-limit           Limit for number of routes handled OSPF process
  router-id             Router ID
  vrrp-state-check      Publish interface via OSPF only if the interface VRRP
                        state is not BACKUP

  clrscr                Clears the display screen
  commit                Commit all changes made in this session
  do                    Run commands from Exec mode
  end                   End current mode and change to EXEC mode
  exit                  End current mode and down to previous mode
  help                  Description of the interactive help system
  revert                Revert changes
```

```
  service             Service Commands
  show                Show running system information
  write               Write running configuration to memory or terminal

rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#
```

router-mode

ROUTER-MODE COMMANDS

Table 22 summarizes router configuration commands.

TABLE 22 OSPF-Router Config Commands

Command	Description	Reference
area	Specifies OSPF enabled interfaces	page 1224
auto-cost	Specifies the reference bandwidth in terms of Mbits per second	page 1230
default-information	Controls the distribution of default information	page 1231
ip	Configures *Internet Protocol* (IP) default gateway priority	page 1232
network	Defines OSPF network settings	page 1233
ospf	Enables OSPF	page 1234
passive	Specifies the configured OSPF interface as passive interface	page 1234
redistribute	Specifies the route types redistributed by OSPF	page 1235
route-limit	Specifies the limit for the number of routes managed by OSPF	page 1236
router-id	Specifies the router ID for OSPF	page 1237
vrrp-state-check	Publishes interface via OSPF based on VRRP status	page 1238
no	Negates a command or sets its defaults	page 1239

area

router-mode

Configures OSPF network area (OSPF enabled interfaces) settings

The following table lists the OSPF Area configuration mode commands.

Command	Description	Reference
area	Creates a new OSPF area and enters its configuration mode	page 1224
OSPF-area-mode	Summarizes OSPF area configuration commands	page 1226

area

area

Configures OSPF network areas (OSPF enables interfaces)

An OSPF network can be subdivided into routing areas to simplify administration and optimize traffic utilization. Areas are logical groupings of hosts and networks, including routers having interfaces connected to an included network. Each area maintains a separate link state database whose information may be summarized towards the rest of the network by the connecting router. Areas are identified by 32-bit IDs, expressed either in decimal, or octet-based dot-decimal notation. Areas can defined as: stub area, totally-stub, non-stub, nssa, totally nssa. Each of these area types have been discussed further in the *area-type* section of this chapter.

At least one default area, bearing number '0', should be configured for every OSPF network. In case of multiple areas, the default area 0 forms the backbone of the network. The default area 0 is used as a link to the other areas. Each area has its own
link-state database.

A router running OSPF sends hello packets to discover neighbors and elect a designated router. The hello packet includes link state information and list of neighbors. OSPF is savvy with layer 2 topologies. If on a point-to-point link, OSPF knows it is sufficient, and the link stays up. If on a broadcast link, the router waits for election before determining if the link is functional.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
area [<0-4294967295>|<IP>]
```

Parameters

```
area [<0-4294967295>|<IP>]
```

<0-4294967295>	Defines an OSPF area in the form of a 32 bit integer. Specify the value from 0 - 4294967295.
<IP>	Defines an OSPF area in the form of an IP address. Specify the IP address.

Example

```
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#area 4 ?

rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.4)#?
Router OSPF Area Mode commands:
  area-type       OSPF area type
  authentication  Authentication scheme for OSPF area
  no              Negate a command or set its defaults
  range           Routes matching this range are considered for summarization
                  (ABR only)

  clrscr          Clears the display screen
  commit          Commit all changes made in this session
  do              Run commands from Exec mode
  end             End current mode and change to EXEC mode
  exit            End current mode and down to previous mode
  help            Description of the interactive help system
  revert          Revert changes
  service         Service Commands
  show            Show running system information
  write           Write running configuration to memory or terminal
```

```
rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.4)#

rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.4)#show
context
  area 0.0.0.4
rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.4)#
```

Related Commands:

no	Removes area configuration settings

OSPF-area-mode

area

The following table summarizes OSPF area mode configuration commands.

Command	Description	Reference
area-type	Configures a particular OSPF area as STUB or NSSA	page 1226
authentication	Specifies the authentication scheme used for the OSPF area	*page 24-1227*
range	Specifies the routes matching address/mask for summarization	page 1228
no	Negates a command or sets its defaults	page 1229

area-type

OSPF-area-mode

Configures a particular OSPF area as STUB, Totally STUB, NSSA or Totally NSSA

Areas can defined as:

- stub area - Is an area that does not receive route advertisements external to the *autonomous system* (AS), and routing from within the area is based entirely on a default route.
- totally-stub - Is an area that does not allow summary routes and external routes. A default route is the only way to route traffic outside of the area. When there is only one route out of the area, fewer routing decisions are needed, lowering system resource utilization.
- non-stub - Is an area that imports autonomous system external routes and forwards to other areas. However. it still cannot receive external routes from other areas.
- nssa - A *Not-So-Stubby Area* (NSSA) is an extension of a stub that allows the injection of limited external routes into a stub area. If selecting NSSA, no external routes, except a default route, enter the area.
- totally-nssa - Is a NSSA using 3 and 4 summary routes are not flooded into this type of area. It is also possible to declare an area both totally stubby and not-so-stubby, which means that the area will receive only the default route from area 0.0.0.0, but can also contain an *Autonomous System Boundary Router* (ASBR) that accepts external routing information and injects it into the local area, and from the local area into area 0.0.0.0.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
area-type [nssa|stub]

area-type nssa {default-cost|no-summary|translate-always|translate-candidate|
          translate-never}

area-type nssa {default-cost <0-16777215> {no-summary}|no-summary
{default-cost
          <0-16777215>}}
area-type nssa {translate-always|translate-candidate|translate-never}
          {(default-cost <0-16777215>|no-summary)}

area-type stub {default-cost <0-16777215> {no-summary}|no-summary
{default-cost
          <0-16777215>}}
```

Parameters

```
area-type [nssa|stub]
```

nssa	Configures the OSPF area as NSSA
stub	Configures the OSPF area as *Stubby Area* (STUB)
default-cost <0-16777215>	Specifies the default summary cost that will be advertised, if the OSPF area is a STUB or NSSA • <0-16777215> – Specify the default summary cost value from 0 - 16777215.
no-summary	Configures the OSPF area as totally STUB if the area-type is STUB or totally NSSA if the area-type is NSSA
translate-always	Always translates type-7 *Link State Advertisements* (LSAs) into type-5 LSAs
translate-candidate	Defines it as default behavior
translate-never	Never translates type-7 LSAs into type-5 LSAs

Example

```
rfs7000-37FABE(config-profile
default-rfs7000-router-ospf-area-0.0.0.1)#area-type stub default-cost 1

rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#show
con
text
  area 0.0.0.1
   area-type stub default-cost 1
rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#
```

Related Commands:

no	Removes configured area-type settings

authentication

OSPF-area-mode

Specifies an authentication scheme used for an OSPF area used with the OSPF dynamic route

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
authentication [message-digest|simple-password]
```

Parameters

```
authentication [message-digest|simple-password]
```

message-digest	Configures the message-digest (MD-5) authentication scheme
simple-password	Configures the simple password authentication scheme

Usage Guidelines:

OSPF packet authentication enables routers to use predefined passwords and participate within a routing domain. The two authentication modes are:

- MD-5 – MD-5 authentication is a cryptographic authentication mode, where every router has a key (password) and key-id configured on it. This key and key-id together form the message digest that is appended to the OSPF packet.
- Simple Password – Simple password authentication allows a password (key) to be configured per area. Routers in the same area and participating in the routing domain have to be configured with the same key.

Example

```
rfs7000-37FABE(config-profile
default-rfs7000-router-ospf-area-0.0.0.1)#authentication simple-password

rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#show
con
text
  area 0.0.0.1
   authentication simple-password
   area-type stub default-cost 1
rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#
```

Related Commands:

no	Removes the authentication scheme

range

OSPF-area-mode

Specifies a range of addresses for routes matching address/mask for OSPF summarization

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
range <IP/M>
```

Parameters

```
range <IP/M>
```

<IP/M>	Specifies the routes matching address/mask for summarization. **NOTE:** This command is applicable for a *Area Border Router* (ABR) only.

Example

```
rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#range
172.16.10.0/24

rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#show
con
text
  area 0.0.0.1
   authentication simple-password
   range 172.16.10.0/24
   area-type stub default-cost 1
rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#
```

Related Commands:

no	Removes the configured network IP range

no

OSPF-area-mode

Negates a command or set its defaults

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
no [area-type|authentication|range]
```

Parameters

```
no [area-type|authentication|range]
```

no <PARAMETER>	Negates a command or set its defaults

Usage Guidelines:

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
The following example shows the OSPF router settings before the ‘no’ commands
are executed:

rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#show
context
  area 0.0.0.1
   authentication simple-password
   range 172.16.10.0/24
   area-type stub default-cost 1
rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#

rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#no
authentication
rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#no
range
 172.16.10.0/24

The following example shows the OSPF router settings after the ‘no’ commands
are executed:

rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#show
context
  area 0.0.0.1
   area-type stub default-cost 1
rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#
```

Related Commands:

area-type	Configures a particular OSPF area as STUB, Totally STUB, NSSA or Totally NSSA
authentication	Specifies the authentication scheme used for an OSPF area
range	Specifies the routes matching address/mask for summarization

auto-cost

router-mode

Configures the reference bandwidth in terms of megabits per second. Specifying the reference bandwidth allows you to control the default metrics for an interface, which is calculated by OSPF.

The formula used to calculate default metrics is: *ref-bw* divided by the *bandwidth*.

Use the ‘no auto-cost reference-bandwidth’ to configure default metrics calculation based on interface type.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
auto-cost reference-bandwidth <1-4294967>
```

Parameters

```
auto-cost reference-bandwidth <1-4294967>
```

reference-bandwidth <1-4294967>	Defines the reference bandwidth in Mbps • <1-4294967> – Specify the reference bandwidth value from1 - 4294967.

Example

```
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#auto-cost
reference-bandwidth 1

Please make sure that auto-cost reference-bandwidth is configured uniformly on
all routers

rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#

rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#show context
 router ospf
  area 0.0.0.4
  auto-cost reference-bandwidth 1
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#
```

Related Commands:

no	Removes auto-cost reference bandwidth settings

default-information

router-mode

Controls the distribution of default route information. Use the *default-information > originate* command to advertise a default route in the routing table.

This option is disabled by default. When enabled, the default route becomes a distributed route.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
default-information originate {always|metric|metric-type}
default-information originate {always|metric <0-16777214>|metric-type [1|2]}
          {(metric <0-16777214>|metric-type[1|2])}
```

Parameters

```
default-information originate {always|metric <0-16777214>|metric-type [1|2]}
{(metric <0-16777214>|metric-type [1|2])}
```

originate	Originates default route information. Enabling this feature makes the default route a distributed route. This option is disabled by default.
always	Optional. Always distributes default route information (will continue to advertise default route information even if that information has been removed from the routing table for some reason). This option is disabled by default.
metric <0-16777214>	This is a recursive parameter and can be optionally configured along with the metric-type option. • metric <0-16777214> – Optional. Specifies OSPF metric value for redistributed routes (this value is used to generate the default route)). Specify a value from 0 - 16777214.

metric-type [1|2]	This is a recursive parameter and can be optionally configured along with the metric option.
	• metric-type [1|2] – Optional. Sets OSPF exterior metric type for redistributed routes (this information is advertised with the OSPF routing domain)
	  • 1 – Sets OSPF external type 1 metrics
	  • 2 – Sets OSPF external type 2 metrics

Example

```
rfs7000-37FABE(config-profile
default-rfs7000-router-ospf)#default-information originate metric-type 2
metric 1

rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#show context
 router ospf
  area 0.0.0.4
  auto-cost reference-bandwidth 1
  default-information originate metric 1 metric-type 2
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#
```

Related Commands:

no	Disables advertising of default route information available in the routing table

ip

router-mode

Configures IP default gateway priority

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
ip default-gateway priority <1-8000>
```

Parameters

```
ip default-gateway priority <1-8000>
```

default-gateway	Configures the default gateway
priority <1-8000>	Sets the priority for the default gateway acquired via OSPF. Specify an integer from 1 - 8000. The default is 7000. **NOTE:** Lower the value, higher is the priority.

Example

```
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#ip default-gateway
priority 1

rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#show context
 router ospf
  area 0.0.0.4
  auto-cost reference-bandwidth 1
  default-information originate metric 1 metric-type 2
  ip default-gateway priority 1
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#
```

Related Commands:

no	Removes default gateway priority settings

network

router-mode

Assigns networks to specified areas (defines the OSPF interfaces and their associated area IDs)

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
network <IP/M> area [<0-4294967295>|<IP>]
```

Parameters

```
network <IP/M> area [<0-4294967295>|<IP>]
```

<IP/M>	Specifies an OSPF network address/mask value. Defines networks (IP addresses and mask) participating in OSPF.
area [<0-4294967295>|<IP>]	Specifies an OSPF area, associated with the OSPF address range, in one of the following formats: • <0-4294967295> – Specifies a 32 bit OSPF area ID from 0 - 4294967295 • <IP> – Defines an OSPF area ID in the form of an IPv4 address

Example

```
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#network 1.2.3.0/24
area 4.5.6.7

rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#show context
```

```
 router ospf
  network 1.2.3.0/24 area 4.5.6.7
  area 0.0.0.4
  auto-cost reference-bandwidth 1
  default-information originate metric 1 metric-type 2
  ip default-gateway priority 1
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#
```

Related Commands:

no	Removes the OSPF network to area ID association

ospf

router-mode

Enables OSPF routing on a profile or device

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
ospf enable
```

Parameters

```
ospf enable
```

ospf enable	Enables OSPF routing on devices using this profile. This option is disabled by default.

Example

```
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#ospf enable

rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#show context
 router ospf
  ospf enable
  network 1.2.3.0/24 area 4.5.6.7
  area 0.0.0.4
  auto-cost reference-bandwidth 1
  default-information originate metric 1 metric-type 2
  ip default-gateway priority 1
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#
```

Related Commands:

no	Disables OSPF routing on a profile or device

passive

router-mode

Configures specified OSPF interface as passive. This option is disabled by default.

A passive interface receives routing updates, but does not transmit them.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
passive [<WORD>|all|vlan <1-4094>]
```

Parameters

```
passive [<WORD>|all|vlan <1-4094>]
```

<WORD>	Enables the OSPF passive mode on the interface specified by the <WORD> parameter
all	Enables the OSPF passive mode on all the L3 interfaces
vlan <1-4094>	Enables the OSPF passive mode on the specified VLAN interface • <1-4094> – Specify the VLAN interface ID from 1 - 4094.

Example

```
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#passive vlan 1

rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#show context
 router ospf
  ospf enable
  network 1.2.3.0/24 area 4.5.6.7
  area 0.0.0.4
  auto-cost reference-bandwidth 1
  default-information originate metric 1 metric-type 2
  passive vlan1
  ip default-gateway priority 1
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#
```

Related Commands:

no	Disables the OSPF passive mode on a specified interface

redistribute

router-mode

Specifies the route types redistributed by OSPF

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
redistribute [connected|kernel|static] {metric <0-16777214>|metric-type [1|2]}
```

Parameters

```
redistribute [connected|kernel|static] {metric <0-16777214>|metric-type [1|2]}
```

connected	Redistributes all connected interface routes by OSPF
kernel	Redistributes all routes that are neither connected, nor static, nor dynamic
static	Redistributes static routes by OSPF
metric <0-16777214>	The following keywords are common to the 'connected', 'kernel', and 'static' parameters: • metric <0-16777214> – Optional. Specifies the OSPF metric value for redistributed routes. • <0-16777214> – Specify a value from 0 - 16777214.
metric-type [1|2]	The following keywords are common to the 'connected', 'kernel', and 'static' parameters: • metric-type [1|2] – Optional. Sets the OSPF exterior metric type for redistributed routes • 1 – Sets the OSPF external type 1 metrics • 2 – Sets the OSPF external type 2 metrics

Example

```
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#redistribute
static metric-type 1

rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#show context
 router ospf
  ospf enable
  network 1.2.3.0/24 area 4.5.6.7
  area 0.0.0.4
  auto-cost reference-bandwidth 1
  default-information originate metric 1 metric-type 2
  redistribute static metric-type 1
  passive vlan1
  ip default-gateway priority 1
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#
```

Related Commands:

no	Removes the OSPF redistribution of various route types

route-limit

router-mode

Limits the number of routes managed by OSPF. The maximum limit supported by the platform is the default configuration defined under the router-ospf context.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
route-limit [num-routes|reset-time|retry-count|retry-timeout]

route-limit [num-routes <DYNAMIC-ROUTE-LIMIT>|reset-time <1-86400>|
          retry-count <1-32>|retry-timeout <1-3600>]
{(num-routes|reset-time|retry-count|
          retry-timeout)}
```

Parameters

```
route-limit [num-routes <DYNAMIC-ROUTE-LIMIT>|reset-time
<1-86400>|retry-count <1-32>|
retry-timeout <1-3600>] {(num-routes|reset-time|retry-count|retry-timeout)}
```

num-routes <DYNAMIC-ROUTE-LIMIT>	Specifies the maximum number of non self-generated *Link State Advertisements* (LSAs) this process can receive • <DYNAMIC-ROUTE-LIMIT> – Specify the dynamic route limit.
reset-time <1-86400>	Specifies the time, in seconds, after which the retry-count is reset to zero. Specify a value from 1 - 86400 seconds. The default is 360 seconds.
retry-count <1-32>	Specifies the maximum number of times adjacencies can be suppressed. Each time OSPF gets into an ignore state, a counter increments. If the counter exceeds the timeout configured by the retry-count parameter, OSPF stays in the same ignore state. Manual intervention is required to get OSPF out of the ignore state. The default is 5.
retry-timeout <1-3600>	Specifies the retry time in seconds. During this time, OSPF remains in ignore state and all adjacencies are suppressed. Specify a value from 1 - 3600 seconds. The default is 60 seconds.

Example

```
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#route-limit
num-routes 10 retry-count 5 retry-timeout 60 reset-time 10

rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#show context
 router ospf
  ospf enable
  network 1.2.3.0/24 area 4.5.6.7
  area 0.0.0.4
  auto-cost reference-bandwidth 1
  default-information originate metric 1 metric-type 2
  redistribute static metric-type 1
  passive vlan1
  route-limit num-routes 10 retry-count 5 retry-timeout 60 reset-time 10
  ip default-gateway priority 1
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#
```

Related Commands:

no	Removes the limit on the number of routes managed by OSPF

router-id

router-mode

Specifies the OSPF router ID

This ID must be established in every OSPF instance. If not explicitly configured, the highest logical IP address is duplicated as the router identifier. However, since the router identifier is not an IP address, it does not have to be a part of any routable subnet in the network.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
router-id <IP>
```

Parameters

```
router-id <IP>
```

<IP>	Identifies the OSPF router by its IP address • <IP> – Specify the router ID in the IP <A.B.C.D> format

Example

```
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#router-id
172.16.10.8

Reload, or execute "clear ip ospf process" command, for this to take effect

rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#
```

Related Commands:

no	Removes the configured OSPF router ID

vrrp-state-check

router-mode

Publishes interface via OSPF based on *Virtual Router Redundancy Protocol* (VRRP) status

VRRP provides automatic assignments of available IP routers to participating hosts. This increases the availability and reliability of routing paths via automatic default gateway selections on an IP subnetwork. This option is enabled by default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
vrrp-state-check
```

Parameters

```
vrrp-state-check
```

vrrp-state-check	Publishes an interface via OSPF based on VRRP status

Example

```
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#vrrp-state-check

Disable and enable OSPF feature for this command to take effect

rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#

rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#show context
include-factory
 router ospf
  ospf enable
  no router-id
  no auto-cost reference-bandwidth
  no default-information originate
  no passive all
  vrrp-state-check
  route-limit num-routes 10 retry-count 5 retry-timeout 60 reset-time 10
  ip default-gateway priority 7000
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#
```

Related Commands:

no	Disables the publishing of an interface via OSPF based on VRRP status

no

router-mode

Negates a command or reverts settings to their default

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
no [area|auto-cost|default-information|ip|network|ospf|passive|redistribute|
          route-limit|router-id|vrrp-state-check]
```

Parameters

```
no [area|auto-cost|default-information|ip|network|ospf|passive|redistribute|
route-limit|router-id|vrrp-state-check]
```

no <PARAMETER>	Negates a command or set its defaults

Usage Guidelines:

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
The following example shows the OSPF router interface settings before the ‘no’
commands are executed:

rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#show context
 router ospf
  network 1.2.3.0/24 area 4.5.6.7
  area 0.0.0.4
  auto-cost reference-bandwidth 1
  default-information originate metric 1 metric-type 2
  redistribute static metric-type 1
  passive vlan1
  route-limit num-routes 10 reset-time 10
  ip default-gateway priority 1
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#

rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#no area 4
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#no auto-cost
reference-bandwidth
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#no network
1.2.3.0/24 area 4.5.6.7

The following example shows the OSPF router interface settings after the ‘no’
commands are executed:

rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#show context
 router ospf
  default-information originate metric 1 metric-type 2
  redistribute static metric-type 1
  passive vlan1
  route-limit num-routes 10 reset-time 10
  ip default-gateway priority 1
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#
```

Related Commands:

area	Configures OSPF network areas (OSPF enables interfaces)
auto-cost	Configures the reference bandwidth in terms of megabits per second
default-information	Controls the distribution of default route information
ip	Configures IP default gateway priority
network	Assigns networks to specified areas
ospf	Enables OSPF
passive	Configures a specified OSPF interface as passive
redistribute	Specifies the route types redistributed by OSPF
route-limit	Limits the number of routes managed by OSPF
router-id	Specifies the router ID for OSPF
vrrp-state-check	Publishes interface via OSPF based on VRRP status

Chapter

ROUTING-POLICY 25

This chapter summarizes routing-policy commands in the CLI command structure.

Routing policies enable network administrators to control data packet routing and forwarding. *Policy-based routing* (PBR) always overrides protocol-based routing. Network administrators can define routing policies based on parameters, such as access lists, packet size etc. For example, a routing policy can be configured to route packets along user-defined routes.

In addition to the above, PBR policies facilitate the provisioning of preferential service to specific traffic. PBR minimally provides the following:

- A means to use source address, protocol, application, and traffic class as traffic routing criteria
- A means to load balance multiple WAN uplinks
- A means to selectively mark traffic for *Quality of Service* (QoS) optimization

Use the (config) instance to configure router-policy commands. To navigate to the (config-routing-policy mode) instance, use the following commands:

<DEVICE>(config)#routing-policy <ROUTING-POLICY-NAME>

```
rfs7000-37FABE(config)#routing-policy testpolicy
rfs7000-37FABE(config)#

rfs7000-37FABE(config-routing-policy-testpolicy)#?
Routing Policy Mode commands:
  apply-to-local-packets  Use Policy Based Routing for packets generated by
                          the device
  logging                 Enable logging for this Route Map
  no                      Negate a command or set its defaults
  route-map               Create a Route Map
  use                     Set setting to use

  clrscr                  Clears the display screen
  commit                  Commit all changes made in this session
  do                      Run commands from Exec mode
  end                     End current mode and change to EXEC mode
  exit                    End current mode and down to previous mode
  help                    Description of the interactive help system
  revert                  Revert changes
  service                 Service Commands
  show                    Show running system information
  write                   Write running configuration to memory or terminal

rfs7000-37FABE(config-routing-policy-testpolicy)#
```

routing-policy-commands

ROUTING-POLICY

Table 23 summarizes routing policy configuration commands.

TABLE 23 Routing-Policy-Config Commands

Command	Description	Reference
apply-to-local-packets	Enables/disables PBR for locally generated packets	page 1242
logging	Enables/disables logging for a specified route map	page 1243
route-map	Creates a route map entry	page 1243
use	Defines default settings to use	page 1252
no	Negates a command or sets its defaults	page 1253
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

apply-to-local-packets

routing-policy-commands

Enables/disables PBR for locally generated packets (packets generated by the device). When enabled, this option implements the match and action clauses defined within route maps. This option is enabled by default.

To disable PBR, use the *no* > *apply-to-local-packets* command.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
apply-to-local-packets
```

Parameters

None

Example

```
rfs7000-37FABE(config-routing-policy-testpolicy)#apply-to-local-packets
rfs7000-37FABE(config-routing-policy-testpolicy)#
```

Related Commands:

no	Disables PBR for locally generated packets

logging

routing-policy-commands

Enables/disables logging for a specified route map. When enabled, this option logs events generated by the enforcement of route-maps. This option is disabled by default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
logging
```

Parameters

None

Example

```
rfs7000-37FABE(config-routing-policy-testpolicy)#logging

rfs7000-37FABE(config-routing-policy-testpolicy)#show context
routing-policy testpolicy
 logging
rfs7000-37FABE(config-routing-policy-testpolicy)#
```

Related Commands:

no	Disables route map logging

route-map

routing-policy-commands

Creates a route map entry and enters the route map configuration mode

In *policy-based routing* (PBR), route maps control the flow of traffic within the network. They override route tables and direct traffic along a specific path.

Route-maps contain a set of filters that select traffic (*match* clauses) and associated actions (*mark* clauses) for routing. Every route-map entry has a precedence value. Lower the precedence, higher is the route-map's priority. All incoming packets are matched against these route-maps entries. The route-map entry with highest precedence (lowest numerical value) is applied first. In case of a

match, action is taken based on the mark clause specified in the route-map. In case of no match, the route-map entry with the next highest precedence is applied. If the incoming packet does not match any of the route-map entries, it is subjected to typical destination-based routing. Each route-map entry can optionally enable/disable logging.

The following criteria can optionally be used as traffic selection segregation criteria:

- *IP Access List* - A typical IP ACL can be used for routing traffic. The mark and log actions in ACL rules however are neglected. Route-map entries have separate logging. Only one ACL can be configured per route map entry.

  ACL rules configured under route map entries merge to create a single ACL. Route map precedence values determine the prioritization of the rules in this merged ACL. An IP DSCP value is also added to the ACL rules.

- *IP DSCP* - Packet filtering can be performed by traffic class, as determined from the IP *Differentiated Services Code Point* (DSCP) field. One DSCP value can be configured per route map entry. If IP ACLs on a WLAN, ports or SVI mark packets, the new/marked DSCP value is used for matching.
- *Incoming WLAN* - Packets can be filtered on the basis of the incoming WLAN. Depending on whether the receiving device has an onboard radio or not, the following two scenarios are possible:
  - Device *with* an onboard radio: If a device having an onboard radio and capable of PBR receives a packet on a local WLAN, this WLAN is used for selection.
  - Device *without* an onboard radio: If a device, without an onboard radio, capable of PBR receives a packet from an extended VLAN, it passes the WLAN information in the MiNT packet to the PBR router. The PBR router uses this information as match criteria.
- *Client role* - The client role can be used as match criteria, similar to a WLAN. Each device has to agree on a unique identifier for role definition and pass the same MINT tunneled packets.
- *Incoming SVI* - A source IP address qualifier in an ACL typically satisfies filter requirements. But if the source host (where the packet originates) is multiple hops away, the incoming SVI can be used as match criteria. In this context the SVI refers to the device interface performing PBR, and not to the source device.

Mark (or action) clauses determine the routing function when a packet satisfies match criteria. If no mark clauses are defined, the default is to fallback to destination-based routing for packets satisfying the match criteria. If no mark clause is configured and fallback to destination-based routing is disabled, then the packet is dropped. The mark clause defines one of following actions:

- *Next hop* - The IP address of the next hop or the outgoing interface through which the packet should be routed. Up to two next hops can be specified. The outgoing interface should be a PPP, a tunnel interface or a SVI which has DHCP client configured. The first reachable hop should be used. But if all next hops are unreachable, typical destination-based route lookup is performed.
- *Default next hop* - If a packet subjected to PBR does not have an explicit route to the destination, the configured default next hop is used. This can be either the IP address of the next hop or the outgoing interface. Only one default next hop can be defined. The difference between the *next hop* and the *default next-hop* is: in case of the former, PBR occurs first, then destination-based routing. In case of the latter, the order is reversed. In both cases:

  .a If a defined next hop is reachable, it is used. If fallback is configured refer to (b).

.b Perform normal destination-based route lookup. If a next hop is found, it is used, if not refer to (c).

.c If default next hop is configured and reachable, it is used, if not, packet is dropped.

- *Fallback* - Enables fallback to destination-based routing if none of the configured next hops are reachable (or not configured). This is enabled by default.
- *Mark IP DSCP* - Configures IP DSCP bits for QoS using an ACL. The mark action of the route maps takes precedence over the mark action of an ACL.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
route-map <1-100>
```

Parameters

```
route-map <1-100>
```

route-map <1-100>	Creates a route map entry and enters the route map configuration mode. Specify a precedence value from 1-100. **NOTE:** Lower the sequence number, higher is the precedence.

Example

```
rfs7000-37FABE(config-routing-policy-testpolicy)#route-map 1

rfs7000-37FABE(config-routing-policy-testpolicy)#show context
routing-policy testpolicy
 logging
 route-map 1
rfs7000-37FABE(config-routing-policy-testpolicy)#

rfs7000-37FABE(config-routing-policy-testpolicy)#route-map 1
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#?
Route Map Mode commands:
  default-next-hop  Default next-hop configuration (aka
                    gateway-of-last-resort)
  fallback          Fallback to destination based routing if no next-hop is
                    configured or all are unreachable
  mark              Mark action for route map
  match             Match clause configuration for Route Map
  next-hop          Next-hop configuration
  no                Negate a command or set its defaults

  clrscr            Clears the display screen
  commit            Commit all changes made in this session
  do                Run commands from Exec mode
  end               End current mode and change to EXEC mode
  exit              End current mode and down to previous mode
```

```
  help              Description of the interactive help system
  revert            Revert changes
  service           Service Commands
  show              Show running system information
  write             Write running configuration to memory or terminal

rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#
```

Related Commands:

no	Removes a route map

route-map-mode

routing-policy-commands

The following table summarizes route-map configuration commands.

Command	Description	Reference
default-next-hop	Sets the default next hop for packets satisfying match criteria	page 1246
fallback	Configures a fallback to the next destination	page 1247
mark	Marks action clause for packets satisfying match criteria	page 1248
match	Sets match clauses for the route map	*page 25-1248*
next-hop	Sets the next hop for packets satisfying match criteria	page 1250
no	Negates a command or sets its default	page 1251

default-next-hop

route-map-mode

Sets the default next hop for packets satisfying match criteria

If a packet, subjected to PBR, does not have an explicit route to the destination, the configured default next hop is used. This value is set as either the IP address of the next hop or the outgoing interface. Only one default next hop can be defined. The difference between the next hop and the default next-hop is: in case of the former, PBR occurs first, then destination-based routing. In case of the latter, the order is reverse. Use this command to set either the default next hop IP address or define either a WWAN1, PPPoE1, or VLAN interface.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
default-next-hop [<IP>|<ROUTER-IF-NAME>|pppoe1|vlan <1-4094>|wwan1]
```

Parameters

```
default-next-hop [<IP>|<ROUTER-IF-NAME>|pppoe1|vlan <1-4094>|wwan1]
```

default-next-hop	Sets the next hop router to which packets are sent in case the next hop is not the adjacent router
<IP>	Specifies next hop router's IP address
<ROUTER-IF-NAME>	Specifies the outgoing interface name (router interface name)
pppoe1	Specifies the PPPoE interface
vlan <1-4094>	Specifies a VLAN interface ID from 1 - 4094
wwan1	Specifies the WAN interface

Example

```
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#default-next-hop
wwan1

rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#show context
 route-map 1
  default-next-hop wwan1
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#
```

Related Commands:

no	Removes default next hop router settings

fallback

route-map-mode

Enables fallback to destination-based routing. This option is enabled by default. To disable fallback, use the *no* > *fallback* command.

The action taken for packets satisfying the match criteria is determined by the mark (action) clauses. If no action is defined, the default is to fallback to destination-based routing.

NOTE
If no mark clause is configured and fallback to destination-based routing is disabled, then the packet is dropped.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
fallback
```

Parameters

None

Example

```
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#fallback
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#
```

Related Commands:

no	Disables fallback to destination-based routing, if no next hop is configured or are unreachable

mark

route-map-mode

Enables the marking of the DSCP field in the IP header

Use this command to set the IP DSCP bits for QoS using an ACL. The mark action of the route maps takes precedence over the mark action of an ACL.

The DSCP field in an IP header enables packet classification. Packet filtering can be done based on traffic class, determined from the IP DSCP field. One DSCP value can be configured per route map entry.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
mark ip dscp <0-63>
```

Parameters

```
mark ip dscp <0-63>
```

ip dscp <0-63>	Marks the DSCP field in the IP header. Specify a DSCP value from 0 - 63.

Example

```
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#mark ip dscp 7

rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#show context
 route-map 1
  default-next-hop wwan1
  mark ip dscp 7
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#
```

Related Commands:

no	Disables marking of IP packets

match

route-map-mode

Sets the match clauses

Each route map entry has a set of *match* clauses used to segregate and filter packets. Packets can be segregated using any one of the following criteria:

- *IP Access List* - A typical IP ACL can be used for routing traffic. The mark and log actions in ACL rules however are neglected. Route-map entries have separate logging. Only one ACL can be configured per route map entry.

  ACL rules configured under route map entries merge to create a single ACL. Route map precedence values determine the prioritization of the rules in this merged ACL. An IP DSCP value is also added to the ACL rules.

- *IP DSCP* - Packet filtering can be performed by traffic class, as determined from the IP *Differentiated Services Code Point* (DSCP) field. One DSCP value can be configured per route map entry. If IP ACLs on a WLAN, ports or SVI mark packets, the new/marked DSCP value is used for matching.
- *Incoming WLAN* - Packets can be filtered on the basis of the incoming WLAN. Depending on whether the receiving device has an onboard radio or not, the following two scenarios are possible:
  - Device *with* an onboard radio: If a device having an onboard radio and capable of PBR receives a packet on a local WLAN, this WLAN is used for selection.
  - Device *without* an onboard radio: If a device, without an onboard radio, capable of PBR receives a packet from an extended VLAN, it passes the WLAN information in the MiNT packet to the PBR router. The PBR router uses this information as match criteria.
- *Client role* - The client role can be used as match criteria, similar to a WLAN. Each device has to agree on a unique identifier for role definition and pass the same MINT tunneled packets.
- *Incoming SVI* - A source IP address qualifier in an ACL typically satisfies filter requirements. But if the source host (where the packet originates) is multiple hops away, the incoming SVI can be used as match criteria. In this context the SVI refers to the device interface performing PBR, and not to the source device.

The action taken for filtered packets is determined by the mark (action) clauses. If no action is defined, the default is to fallback to destination-based routing for packets satisfying the match criteria. For more information on configuring mark clauses, see *mark*. And for more information on fallback action, see *fallback*.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
match [incoming-interface|ip|ip-access-list|wireless-client-role|wlan]

match incoming-interface [<ROUTER-IF-NAME>|pppoe1|vlan <1-4094>|wwan1]
match ip dscp <0-63>
match ip-access-list <IP-ACCESS-LIST-NAME>
match wireless-client-role <ROLE-POLICY-NAME> <ROLE-NAME>
match wlan <WLAN-NAME>
```

Parameters

`match incoming-interface [<ROUTER-IF-NAME>|pppoe1|vlan <1-4094>|wwan1]`

incoming-interface	Sets the incoming SVI match clause. Specify an interface name.
<ROUTER-IF-NAME>	Specifies the layer 3 interface name (route interface)
pppoe1	Specifies the PPP over Ethernet interface
vlan <1-4094>	Specifies the VLAN interface. Specify a VLAN ID from 1 - 4094.
wwan1	Specifies the WAN interface name

`match ip dscp <0-63>`

ip dscp <0-63>	Sets the DSCP match clause. Specify a value from 0 - 63. The defined DSCP value is used as a matching clause for this route map.

`match ip-access-list <IP-ACCESS-LIST-NAME>`

ip-access-list <IP-ACCESS-LIST-NAME>	Sets the match clause using a pre-configured IP access list. Specify a pre-configured IP access list name.

`match wireless-client-role <ROLE-POLICY-NAME> <ROLE-NAME>`

wireless-client-role <ROLE-POLICY-NAME> <ROLE-NAME>	Sets the wireless client role match clause. Specify a pre-configured role policy and a pre-configured role within it.

`match wlan <WLAN-NAME>`

wlan <WLAN-NAME>	Sets the incoming WLAN match clause. Specify a WLAN name.

Example

```
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#match
incoming-interface pppoe1

rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#show context
 route-map 1
  match incoming-interface pppoe1
  default-next-hop wwan1
  mark ip dscp 7
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#
```

Related Commands:

no	Disables match clause settings for this route map

next-hop

route-map-mode

Sets the next hop for packets satisfying match criteria

This command allows you to configure the primary and secondary hop priority requests.

Define the primary and secondary hop settings. When defined, the primary hop resource is used with no additional considerations when ever it is available.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
next-hop [<IP>|<ROUTER-IF-NAME>|pppoe1|vlan <1-4094>|wwlan1]
          {<IP>|<ROUTER-IF-NAME>|pppoe1|vlan <1-4094>|wwlan1}
```

Parameters

```
next-hop [<IP>|<ROUTER-IF-NAME>|pppoe1|vlan <1-4094>|wwlan1]
{<IP>|<ROUTER-IF-NAME>|pppoe1|vlan <1-4094>|wwlan1}
```

next-hop	Sets the next hop (primary and secondary) for packets satisfying match criteria It is not mandatory to define the secondary hop interface. The secondary hop is used in case the primary hop is unavailable.
<IP>	Specifies the primary and secondary next hop router's IP address
<WORD>	Specifies the layer 3 Interface name (router interface)
pppoe1	Specifies the PPP over Ethernet interface
vlan <1-4094>	Specifies the VLAN interface. Specify a VLAN ID from 1 - 4094. The VLAN interface should be a DHCP client.
wwan1	Specifies the WAN interface

Example

```
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#next-hop vlan 1

rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#show context
 route-map 1
  match incoming-interface pppoe1
  next-hop vlan1
  default-next-hop wwan1
  mark ip dscp 7
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#
```

Related Commands:

no	Disables the next hop router settings

no

route-map-mode

Negates a command or sets its defaults

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no [default-next-hop|fallback|mark|match|next-hop]
```

Parameters

```
no [default-next-hop|fallback|mark|match|next-hop]
```

no <PARAMETER>	Negates a command or set its defaults

Usage Guidelines:

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
The following example shows the route-map ‘1’ settings before the ‘no’
commands are executed:

rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#show context
 route-map 1
  match incoming-interface pppoe1
  next-hop vlan1
  default-next-hop wwan1
  mark ip dscp 7
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#

rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#no
default-next-hop
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#no next-hop

The following example shows the route-map ‘1’ settings after the ‘no’ commands
are executed:

rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#show context
 route-map 1
  match incoming-interface pppoe1
  mark ip dscp 7
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#
```

Related Commands:

default-next-hop	Sets the next hop for packets satisfying match criteria
fallback	Configures a fallback to the next destination
mark	Marks an action for a route map
match	Sets match clauses for a route map
next-hop	Sets the next hop for packets satisfying match criteria

use

routing-policy-commands

Uses *Critical Resource Management* (CRM) to monitor link status

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
use critical-resource-monitoring
```

Parameters

```
use critical-resource-monitoring
```

use critical-resource-monitoring	Uses CRM to monitor the status of a link. Selecting this option determines the disposition of the route-map next hop via monitored critical resources. Link monitoring is the function used to determine a potential fail over to the secondary next hop. This option is enabled by default.

Example

```
rfs7000-37FABE(config-routing-policy-testpolicy)#use
critical-resource-monitoring
rfs7000-37FABE(config-routing-policy-testpolicy)#
```

Related Commands:

no	Disables CRM link status monitoring

no

routing-policy-commands

Negates a command or sets its defaults

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no [apply-to-local-packets|logging|route-map|use]
```

Parameters

```
no [apply-to-local-packets|logging|route-map|use]
```

no <PARAMETER>	Negates a command or set its defaults

Usage Guidelines:

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
The following example shows the routing policy ‘testpolicy’ settings before
the ‘no’ commands are executed:

rfs7000-37FABE(config-routing-policy-testpolicy)#show context
routing-policy testpolicy
 logging
 route-map 1
  match incoming-interface pppoe1
  default-next-hop wwan1  mark ip dscp 7
rfs7000-37FABE(config-routing-policy-testpolicy)#

rfs7000-37FABE(config-routing-policy-testpolicy)#no logging
rfs7000-37FABE(config-routing-policy-testpolicy)#no route-map 1
rfs7000-37FABE(config-routing-policy-testpolicy)#no apply-to-local-packets

The following example shows the routing policy ‘testpolicy’ settings after the
‘no’ commands are executed:

rfs7000-37FABE(config-routing-policy-testpolicy)#show context
routing-policy testpolicy
 no apply-to-local-packets
rfs7000-37FABE(config-routing-policy-testpolicy)#
```

Related Commands:

apply-to-local-packets	Enables/disables PBR for locally generated packets
logging	Enables logging for a specified route map
route-map	Creates a route map entry and enters the route map configuration mode
use	Uses CRM to monitor the status of a link

Chapter

AAA-TACACS-POLICY 26

This chapter summarizes the *accounting, authentication, and authorization* (AAA) *Terminal Access Control Access-Control System* (TACACS) policy commands in the CLI command structure.

TACACS is a network security application that provides additional network security by providing a centralized authentication, authorization, and accounting platform. TACACS implementation requires configuration of the TACACS authentication server and database.

Use the (config) instance to configure AAA-TACACS policy commands. To navigate to the config-aaa-tacacs-policy instance, use the following commands:

```
<DEVICE>(config)#aaa-tacacs-policy <POLICY-NAME>

rfs7000-37FABE(config)#aaa-tacacs-policy test
rfs7000-37FABE(config-aaa-tacacs-policy-test)#?
AAA TACACS Policy Mode commands:
  accounting      Configure accounting parameters
  authentication  Configure authentication parameters
  authorization   Configure authorization parameters
  no              Negate a command or set its defaults

  clrscr          Clears the display screen
  commit          Commit all changes made in this session
  do              Run commands from Exec mode
  end             End current mode and change to EXEC mode
  exit            End current mode and down to previous mode
  help            Description of the interactive help system
  revert          Revert changes
  service         Service Commands
  show            Show running system information
  write           Write running configuration to memory or terminal

rfs7000-37FABE(config-aaa-tacacs-policy-test)#
```

aaa-tacacs-policy

AAA-TACACS-POLICY

Table 24 summarizes AAA-TACACS policy configuration commands.

TABLE 24 AAA-TACACS-Policy-Config Commands

Command	Description	Reference
accounting	Configures TACACS accounting parameters	page 1256
authentication	Configures TACACS authentication parameters	page 1258
authorization	Configures TACACS authorization parameters	page 1260
no	Negates a command or sets its default	page 1263
clrscr	Clears the display screen	page 385

TABLE 24 AAA-TACACS-Policy-Config Commands

Command	Description	Reference
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

accounting

aaa-tacacs-policy

Configures the server type and interval at which interim accounting updates are sent to the server. Up to 2 accounting servers can be configured.

This feature tracks user activities on the network, and provides information such as, resources used and usage time. This information can be used for audit and billing purposes.

TACACS accounting tracks user activity and is useful for security audit purposes.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
accounting [access-method|auth-fail|commands|server|session]

accounting access-method [all|console|ssh|telnet] {(console|ssh|telnet)}

accounting [auth-fail|commands|session]

accounting server [<1-2>|preference]

accounting server preference
[authenticated-server-host|authenticated-server-number|
          authorized-server-host|authorized-server-number|none]

accounting server <1-2> [host|retry-timeout-factor <50-200>|timeout]
accounting server <1-2> host <IP/HOSTNAME> {secret [0 <SECRET>|2
<SECRET>|<SECRET>]}
          {port <1-65535>}
accounting server <1-2> timeout <3-5> {attempts <1-3>}
```

Parameters

`accounting access-method [all|console|ssh|telnet]` *`{(console|ssh|telnet)}`*

access-method	Configures TACACS accounting access mode. The options are: console, SSH, Telnet, and all
all	Configures TACACS accounting for all access modes
console	Configures TACACS accounting for console access only
ssh	Configures TACACS accounting for SSH access only
telnet	Configures TACACS accounting for Telnet access only

`accounting [auth-fail|commands|session]`

auth-fail	Enables accounting for authentication fail details. This option is disabled by default.
commands	Enables accounting of commands executed. This option is disabled by default.
session	Enables accounting for session start and stop details. This option is disabled by default.

`accounting server preference [authenticated-server-host|authenticated-server-number| authorized-server-host|authorized-server-number|none]`

server	Configures a TACACS accounting server
preference	Configures the accounting server preference (specifies the method of selecting a server, from the pool, to send the request)
authenticated-server-host	Sets the authentication server as the accounting server. This is the default setting. This parameter indicates the same server is used for authentication and accounting. The server is referred to by its hostname.
authenticated-server-number	Sets the authentication server as the accounting server This parameter indicates the same server is used for authentication and accounting. The server is referred to by its index or number.
authorized-server-host	Sets the authorization server as the accounting server This parameter indicates the same server is used for authorization and accounting. The server is referred to by its hostname.
authorized-server-number	Sets the authorized server as the accounting server This parameter indicates the same server is used for authorization and accounting. The server is referred to by its index number.
none	Indicates the accounting server is independent of the authentication and authorization servers

`accounting server <1-2> retry-timeout-factor <50-200>`

server <1-2>	Configures an accounting server. Up to 2 accounting servers can be configured
retry-timeout-factor <50-200>	Sets the scaling factor for retry timeouts • <50-200> – Specify a value from 50 - 200. The default 15 100. A value of 100 indicates the time gap between two consecutive retires remains the same irrespective of the number of retries. A value lesser than 100 indicates the time gap between two consecutive retries reduces with each successive retry. A value greater than 100 indicates the time gap between two consecutive retries increases with each successive retry.

`accounting server <1-2> host <IP/HOSTNAME> {secret [0 <SECRET>|2 <SECRET>|<SECRET>]} {port <1-65535>}`

server <1-2>	Configures an accounting server. Up to 2 accounting servers can be configured
host <IP/HOSTNAME>	Configures the accounting server's IP address or hostname
secret [0 <SECRET>| 2 <SECRET>|<SECRET>]	Optional. Configures a common secret key used to authenticate with the accounting server • 0 <SECRET> – Configures a clear text secret key • 2 <SECRET> – Configures an encrypted secret key • <SECRET> – Specify the secret key. This shared secret should not exceed 127 characters.
port <1-65535>	Optional. Configures the accounting server port (the port used to connect to the accounting server) • <1-65535> – Specify the TCP accounting port number from 1 - 65535. The default port is 49.

`accounting server <1-2> timeout <3-5> {attempts <1-3>}`

server <1-2>	Configures an accounting server. Up to 2 accounting servers can be configured
timeout <3-5>	Configures the timeout for each request sent to the TACACS accounting server. This is the time allowed to elapse before another request is sent to the TACACS accounting server. If a response is received from the server within this time, no retry is attempted. • <3-5> – Specify a value from 3 - 5 seconds. The default is 3 seconds.
attempts <1-3>	Optional. Specifies the number of times a transmission request is attempted. This is the maximum number of times a request is sent to the TACACS accounting server before getting discarded. • <1-3> – Specify a value from 1 - 3. The default is 3.

Example

```
rfs7000-37FABE(config-aaa-tacacs-policy-test)#accounting auth-fail

rfs7000-37FABE(config-aaa-tacacs-policy-test)#accounting commands

rfs7000-37FABE(config-aaa-tacacs-policy-test)#accounting server preference
authorized-server-number

rfs7000-37FABE(config-aaa-tacacs-policy-test)#show context
aaa-tacacs-policy test
 accounting server preference authorized-server-number
 accounting auth-fail
 accounting commands
rfs7000-37FABE(config-aaa-tacacs-policy-test)#
```

Related Commands:

no	Resets values or disables commands

authentication

aaa-tacacs-policy

Configures user authentication parameters. Users are allowed or denied access to the network based on the authentication parameters set.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
authentication [access-method|directed-request|server|service]

authentication access-method [all|console|ssh|telnet|web]
{(console|ssh|telnet|web)}

authentication directed-request

authentication server <1-2> [host|retry-timeout-factor|timeout]
authentication server <1-2> host <IP/HOSTNAME> {secret [0 <SECRET>|2
<SECRET>|<SECRET>]}
          {port <1-65535>}
authentication server <1-2> retry-timeout-factor <50-200>
authentication server <1-2> timeout <3-60> {attempts <1-10>}

authentication service <SERVICE-NAME> {protocol <AUTHENTICATION-PROTO-NAME>}
```

Parameters

```
authentication access-method [all|console|ssh|telnet|web]
{(console|ssh|telnet)}
```

access-method	Configures access modes for TACACS authentication. The options are: console, SSH, Telnet, Web, and all
all	Authenticates users using all access modes (console, SSH, and Telnet)
console	Authenticates users using console access only
ssh	Authenticates users using SSH access only
telnet	Authenticates users using Telnet access only
web	Authenticates users using Web interface only

```
authentication directed-request
```

directed-request	Enables user to specify TACACS server to use with `@server'. This option is disabled by default. The specified server should be present in the configured servers list.

```
authentication server <1-2> host <IP/HOSTNAME> {secret [0 <SECRET>|2 <SECRET>|
<SECRET>]} {port <1-65535>}
```

server <1-2>	Configures a TACACS authentication server. Up to 2 TACACS servers can be configured • <1-2> – Specify the TACACS server index from 1 - 2.
host <IP/HOSTNAME>	Sets the TACACS server's IP address or hostname
secret [0 <SECRET>| 2 <SECRET>|<SECRET>]	Configures the secret key used to authenticate with the TACACS server • 0 <SECRET> – Configures a clear text secret • 2 <SECRET> – Configures an encrypted secret • <SECRET> – Specify the secret key. The shared key should not exceed 127 characters.
port <1-65535>	Optional. Specifies the port used to connect to the TACACS server • <1-65535> – Specify a value for the TCP authentication port from 1 - 65535. The default port is 49.

`authentication server <1-2> retry-timeout-factor <50-200>`

server <1-2>	Configures a TACACS authentication server. Up to 2 TACACS servers can be configured • <1-2> – Specify the TACACS server index from 1 - 2.
retry-timeout-factor <50-200>	Configures timeout scaling between two consecutive TACACS authentication retries • <50-200> – Specify the scaling factor from 50 - 200. The default is 100. A value of 100 indicates the interval between consecutive retires remains the same irrespective of the number of retries. A value lesser than 100 indicates the interval between consecutive retries reduces with each successive retry. A value greater than 100 indicates the interval between consecutive retries increases with each successive retry.

`authentication server <1-2> timeout <3-60> {attempts <1-10>}`

server <1-2>	Configures a TACACS authentication server. Up to 2 TACACS servers can be configured • <1-2> – Specify the TACACS server index from 1- 2.
timeout <3-60>	Configures the timeout, in seconds, for each request sent to the TACACS server. This is the time allowed to elapse before another request is sent to the TACACS server. If a response is received from the TACACS server within this time, no retry is attempted. • <3-60> – Specify a value from 3- 60 seconds. The default is 3 seconds.
attempts <1-10>	Optional. Indicates the number of retry attempts to make before giving up • <1-10> – Specify a value from 1 -10. The default is 3.

`authentication service <SERVICE-NAME> {protocol <AUTHENTICATION-PROTO-NAME>}`

service <SERVICE-NAME>	Configures the TACACS authentication service name
protocol <AUTHENTICATION-PROTO-NAME>	Optional. Specify the authentication protocol used with this TACACS policy. A maximum of five entries is allowed.

Example

```
rfs7000-37FABE(config-aaa-tacacs-policy-test)#authentication directed-request

rfs7000-37FABE(config-aaa-tacacs-policy-test)#show context
aaa-tacacs-policy test
 authentication directed-request
 accounting server preference authorized-server-number
 accounting auth-fail
 accounting commands
rfs7000-37FABE(config-aaa-tacacs-policy-test)#
```

Related Commands:

no	Resets values or disables commands

authorization

aaa-tacacs-policy

Configures authorization parameters

This feature allows network administrators to limit user accessibility and configure varying levels of accessibility for different users.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
authorization [access-method|allow-privileged-commands|server]

authorization access-method [all|console|telnet|ssh] {(console|ssh|telnet)}

authorization server [<1-2>|preference]

authorization server <1-2> [host|retry-timeout-factor|timeout]
authorizationserver <1-2> host <IP/HOSTNAME> {secret [0 <SECRET>|2
<SECRET>|<SECRET>]}
          {port <1-65535>}

authorization server <1-2> retry-timeout-factor <50-200>
authorization server <1-2> timeout <3-5> {attempts <1-3>}
authorization server preference
[authenticated-server-host|authenticated-server-
          number|none]
```

Parameters

`authorization access-method [all|console|telnet|ssh] {(console|ssh|telnet)}`

access-method	Configures the access method for command authorization
all	Authorizes commands from all access methods
console	Authorizes commands from the console only
telnet	Authorizes commands from Telnet only
ssh	Authorizes commands from SSH only
{console|ssh|telnet}	Optional. Configures more than one access method for command authorization.

`authorization allow-privileged-commands`

allow-privileged-commands	Allows privileged commands execution without command authorization. This option is disabled by default.

`authorization server <1-2> host <IP/HOSTNAME> {secret [0 <SECRET>|2 <SECRET>|<SECRET>]} {port <1-65535>}`

server <1-2>	Configures a TACACS authorization server. Up to 2 TACACS servers can be configured • <1-2> – Specify the TACACS server index from 1 - 2.
host <IP/HOSTNAME>	Sets the TACACS server's IP address or hostname

secret [0 <SECRET>| 2 <SECRET>|<SECRET>]	Optional. Configures the secret used to authorize with the TACACS server • 0 <SECRET> – Configures a clear text secret • 2 <SECRET> – Configures an encrypted secret • <SECRET> – Specify the secret key. The shared key should not exceed 127 characters.
port <1-65535>	Optional. Specifies the port used to connect to the TACACS server • <1-65535> – Specify a value for the TCP authorization port from 1 - 65535. The default port is 49.

```
authorization server <1-2> retry-timeout-factor <50-200>
```

server <1-2>	Configures a TACACS authorization server. Up to 2 TACACS servers can be configured • <1-2> – Specify the TACACS server index from 1 - 2.
retry-timeout-factor <50-200>	Configures the scaling of timeouts between consecutive TACACS authorization retries • <50-200> – Specify the scaling factor from 50 - 200. The default is 100. A value of 100 indicates the interval between consecutive retires remains the same irrespective of the number of retries. A value lesser than 100 indicates the interval between consecutive retries reduces with each successive retry. A value greater than 100 indicates the interval between consecutive retries increases with each successive retry.

```
authorization server <1-2> timeout <3-5> {attempts <1-3>}
```

server <1-2>	Configures a TACACS authorization server. Up to 2 TACACS servers can be configured • <1-2> – Specify the TACACS server's index from 1- 2.
timeout <3-5>	Configures the timeout, in seconds, for each request sent to the TACACS server. This is the time allowed to elapse before another request is sent to the TACACS server. If a response is received from the TACACS server within this time, no retry is attempted. • <3-5> – Specify a value from 3 - 5 seconds. The default is 3 seconds.
attempts <1-3>	Optional. Indicates the number of retry attempts to make before giving up • <1-3> – Specify a value from 1 - 3. The default is 3.

```
authorization server preference
[authenticated-server-host|authenticated-server-number|none]
```

preference	Configures the authorization server preference
authenticated-server-host	Sets the authentication server as the authorization server This parameter indicates the same server is used for authentication and authorization+. The server is referred to by its hostname.
authenticated-server-number	Sets the authentication server as the authorization server This parameter indicates the same server is used for authentication and authorization. The server is referred to by its index or number.
none	Indicates the authorization server is independent of the authentication

Example

```
rfs7000-37FABE(config-aaa-tacacs-policy-test)#authorization
allow-privileged-commands

rfs7000-37FABE(config-aaa-tacacs-policy-test)#show context
aaa-tacacs-policy test
 authentication directed-request
 accounting server preference authorized-server-number
 authorization allow-privileged-commands
 accounting auth-fail
 accounting commands
```

```
rfs7000-37FABE(config-aaa-tacacs-policy-test)#
```

Related Commands:

no	Resets values or disables commands

no

aaa-tacacs-policy

Negates a AAA TACACS policy command or sets its default

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no [accounting|authentication|authorization]
```

Parameters

```
no <PARAMETER>
```

no <PARAMETER>	Provide the parameters needed to reset or disable the desired AAA-TACACS policy setting.

Example

```
The following example shows the AAA-TACACS policy ‘test’ settings before the
‘no’ commands are executed:

rfs7000-37FABE(config-aaa-tacacs-policy-test)#show context
aaa-tacacs-policy test
 authentication directed-request
 accounting server preference authorized-server-number
 authorization allow-privileged-commands
 accounting auth-fail
 accounting commands
rfs7000-37FABE(config-aaa-tacacs-policy-test)#

rfs7000-37FABE(config-aaa-tacacs-policy-test)#no authentication
directed-request
rfs7000-37FABE(config-aaa-tacacs-policy-test)#no accounting auth-fail
rfs7000-37FABE(config-aaa-tacacs-policy-test)#no authorization
allow-privileged-
commands

The following example shows the AAA-TACACS policy ‘test’ settings after the
‘no’ commands are executed:

rfs7000-37FABE(config-aaa-tacacs-policy-test)#show context
aaa-tacacs-policy test
 accounting server preference authorized-server-number
```

```
 accounting commands
rfs7000-37FABE(config-aaa-tacacs-policy-test)#
```

Related Commands:

accounting	Configures TACACS accounting parameters
authentication	Configures TACACS authentication parameters
authorization	Configures TACACS authorization parameters

Chapter

MESHPOINT

27

This chapter summarizes the Meshpoint commands in the CLI command structure.

Meshpoints are detector radios that monitor their coverage areas for potential failed peers or coverage area holes requiring transmission adjustments for coverage compensation.

This chapter is organized as follows:

meshpoint-config-instance

MESHPOINT

MeshConnex (MCX) is a mesh networking technology that is comparable to the 802.11s mesh networking specification. MCX meshing uses a hybrid proactive/on-demand path selection protocol, similar to *Ad hoc On Demand Distance Vector* (AODV) routing protocols. This allows it to form efficient paths using multiple attachment points to a distribution WAN, or form purely ad-hoc peer-to-peer mesh networks in the absence of a WAN. Each device in the MCX mesh proactively manages its own path to the distribution WAN, but can also form peer-to-peer paths on demand to improve forwarding efficiency.

MCX is not compatible with MiNT Based meshing, though the two technologies can be enabled simultaneously in certain circumstances.

MCX is designed for large-scale, high-mobility outdoor mesh deployments. MCX continually gathers data from beacons and transmission attempts to estimate the efficiency and throughput of each MP-to-MP link. MCX uses this data to dynamically form and continually maintain paths for forwarding network frames.

In MCX systems, a *meshpoint* (MP) is a virtual mesh networking instance on a device, similar to a WLAN AP. On each device, up to 4 MPs can be created and 2 can be created per radio. MPs can be configured to use one or both radios in the device. If the MP is configured to use both radios, the path selection protocols will continually select the best radio to reach each destination. Each MP participates in a single Mesh Network, defined by the MeshID. The MeshID is typically a descriptive network name, similar to the SSID of a WLAN. All MPs configured to use the same MeshID attempt to form a mesh and interoperate. The MeshID allows overlapping mesh networks to discriminate and disregard MPs belonging to different networks.

Use the (config) instance to configure a meshpoint. To navigate to the meshpoint configuration instance, use the following command:

```
<DEVICE>(config)#meshpoint <MESHPOINT-NAME>

rfs7000-37FABE(config)#meshpoint test
rfs7000-37FABE(config-meshpoint-test)#
```

```
rfs7000-37FABE(config-meshpoint-test)#?
Mesh Point Mode commands:
  allowed-vlans  Set the allowed VLANs
  beacon-format  The beacon format of this meshpoint
  control-vlan   VLAN for meshpoint control traffic
  data-rates     Specify the 802.11 rates to be supported on this meshpoint
  description    Configure a description of the usage of this meshpoint
  meshid         Configure the Service Set Identifier for this meshpoint
  neighbor       Configure neighbor specific parameters
  no             Negate a command or set its defaults
  root           Set this meshpoint as root
  security-mode  The security mode of this meshpoint
  shutdown       Shutdown this meshpoint
  use            Set setting to use
  wpa2           Modify ccmp wpa2 related parameters

  clrscr         Clears the display screen
  commit         Commit all changes made in this session
  do             Run commands from Exec mode
  end            End current mode and change to EXEC mode
  exit           End current mode and down to previous mode
  help           Description of the interactive help system
  revert         Revert changes
  service        Service Commands
  show           Show running system information
  write          Write running configuration to memory or terminal

rfs7000-37FABE(config-meshpoint-test)#
```

The following table summarizes meshpoint configuration commands.

TABLE 25 Meshpoint-Config commands

Command	Description	Reference
allowed-vlans	Configures VLANs allowed on the meshpoint	page 1267
beacon-format	Configures the beacon format for the meshpoint AP	page 1268
control-vlan	Configures the VLAN where meshpoint control traffic traverses	page 1269
data-rates	Configures the data rates supported per frequency band	page 1269
description	Configures a human friendly description for this meshpoint	page 1273
meshid	Configures a unique ID for this meshpoint	page 1274
neighbor	Configures the neighbor inactivity time out for this meshpoint	page 1274
no	Negates a command or reverts settings to their default	page 1275
root	Configures a meshpoint as the root meshpoint	page 1278
security-mode	Configures the security mode on the meshpoint.	page 1279
service	Allows only 802.11n capable neighbors to create a mesh connection	page 1280
shutdown	Shuts down the meshpoint	page 1281
use	Configures a QoS policy for use with this meshpoint	page 1281
wpa2	Configures WPA2 encryption settings	page 1282
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234

TABLE 25 Meshpoint-Config commands

Command	Description	Reference
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

allowed-vlans

meshpoint-config-instance

Defines VLANs allowed on the mesh network. A VLAN must be added to the allowed VLANs list for data to be allowed across the mesh network. Use this command to remove VLANs from the list of allowed VLANs.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
allowed-vlans [<VLAN-ID>|add <VLAN-ID>|remove <VLAN-ID>]
```

Parameters

```
allowed-vlans [<VLAN-ID>|add <VLAN-ID>|remove <VLAN-ID>]
```

allowed-vlans	Defines VLANs allowed access on the mesh network
<VLAN-ID>	The VLAN ID or the range of IDs to be managed. A single VLAN or multiple VLANs can be added to the list of allowed VLANs. When adding multiple VLANs, specify the range (for example, 10-20, 25, 30-35). Use this command to create a VLAN list on a new meshpoint.
add <VLAN>	Adds a single VLAN or a range of VLANs to the list of allowed VLANs. To specify a range of VLANs, specify the first and last VLAN ID in the range separated by a hyphen (for example, 1-10).
remove <VLAN>	Removes a single VLAN or a range of VLANs from the list of allowed VLANs.

Example

```
rfs7000-37FABE(config-meshpoint-test)#allowed-vlans 1

rfs7000-37FABE(config-meshpoint-test)#allowed-vlans add 10-23

rfs7000-37FABE(config-meshpoint-test)#allowed-vlans remove 17
```

```
rfs7000-37FABE(config-meshpoint-test)#show context
meshpoint test
 meshid test
 beacon-format mesh-point
 control-vlan 1
 allowed-vlans 1,10-16,18-23
 security-mode none
 no root
rfs7000-37FABE(config-meshpoint-test)#
```

Related Commands:

no	Clears the list of VLANs allowed access to the mesh network

beacon-format

meshpoint-config-instance

Configures the beacon transmission format for this meshpoint. Beacons are transmitted periodically to advertise that a wireless network is available. It contains all the required information for a device to connect to the network.

The beacon format advertises how a mesh capable Brocade Mobility 71XX Access Point acts. APs can act either as an access point or a meshpoint.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
beacon-format [access-point|mesh-point]
```

Parameters

```
beacon-format [access-point|mesh-point]
```

beacon-format	Configures how a mesh capable AP71XX acts in a mesh network
access-point	Uses access point style beacons
mesh-point	Uses meshpoint style beacons (this is the default setting)

Example

```
rfs7000-37FABE(config-meshpoint-test)#beacon-format mesh-point

rfs7000-37FABE(config-meshpoint-test)#show context
meshpoint test
 meshid test
 beacon-format mesh-point
 control-vlan 1
 allowed-vlans 1,10-16,18-23
 security-mode none
```

```
 no root
rfs7000-37FABE(config-meshpoint-test)#
```

Related Commands:

no	Resets the beacon format for this meshpoint to its default (mesh-point)

control-vlan

meshpoint-config-instance

Mesh management traffic can be sent over a dedicated VLAN. This dedicated VLAN is known as a control VLAN. This command configures a VLAN as the dedicated control VLAN.

Supported in the following platforms:

- Access Points — Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Access Points (as root APs only) — Brocade Mobility 650 Access Point
- Wireless Controllers — Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
control-vlan <1-4094>
```

Parameters

```
control-vlan <1-4094>
```

control-vlan	Configures a VLAN as a dedicated carrier of mesh management traffic
<1-4094>	The VLAN used as the control VLAN. The default is VLAN 1.

Example

```
rfs7000-37FABE(config-meshpoint-test)#control-vlan 1

rfs7000-37FABE(config-meshpoint-test)#show context
meshpoint test
 meshid test
 beacon-format mesh-point
 control-vlan 1
 allowed-vlans 1,10-16,18-23
 security-mode none
 no root
rfs7000-37FABE(config-meshpoint-test)#
```

Related Commands:

no	Resets the control VLAN for this meshpoint to its default of 1

data-rates

meshpoint-config-instance

Configures individual data rates for the 2.4 GHz and 5.0 GHz frequency bands

Supported in the following platforms:

- Access Points — Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Access Points (as root APs only) — Brocade Mobility 650 Access Point
- Wireless Controllers — Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
data-rates [2.4GHz|5GHz]

data-rates 2.4GHz [b-only|bg|bgn|default|g-only|gn]
data-rates 2.4GHz custom (1|11|12|18|2|24|36|48|5.5|54|6|9|basic-1|basic-11|

basic-12|basic-18|basic-2|basic-24|basic-36|basic-48|basic-5.5|basic-54|basic
-6|
          basic-9|mcs0-15|mcs0-7|mcs8-15|basic-mcs0-7)

data-rates 5GHz [a-only|an|default]
data-rates 5GHz custom
(12|18|24|36|48|54|6|9|basic-1|basic-11|basic-12|basic-18|

basic-2|basic-24|basic-36|basic-48|basic-5.5|basic-54|basic-6|basic-9|mcs0-15
|
          mcs0-7|mcs8-15|basic-mcs0-7)
```

Parameters

```
data-rates 2.4GHz [b-only|bg|bgn|default|g-only|gn]
```

data-rates 2.4GHz	Configures preset data rates for the 2.4 GHz frequency.
b-only	Configures data rate for the meshpoint using 802.11b only rates.
bg	Configures data rate for the meshpoint using 802.11b and 802.11g rates.
default	Configures data rate for the meshpoint at a pre-configured default rate for this frequency.
g-only	Configures data rate for the meshpoint using 802.11g only rates.
gn	Configures data rate for the meshpoint using 802.11g and 802.11n rates.

```
data-rates 2.4GHz custom [1|11|12|18|2|24|36|48|5.5|54|6|9|basic-1|basic-11|
basic-12|basic-18|basic-2|basic-24|basic-36|basic-48|basic-5.5|basic-54 |
basic-6|basic-9|mcs0-15|mcs0-7|mcs8-15|basic-mcs0-7]
```

data-rates 2.4GHz	Configures the preset data rates for the 2.4 GHz frequency Define both minimum *Basic* and optimal *Supported* rates as required for the 802.11b rates, 802.11g rates and 802.11n rates supported by the 2.4 GHz band. These are the rates wireless client traffic is supported within this mesh point. If supporting 802.11n, select a supported MCS index. Set a *Modulation and Coding Scheme* (MCS) in respect to the radio's channel width and guard interval. A MCS defines (based on RF channel conditions) an optimal combination of 8 data rates, bonded channels, multiple spatial streams, different guard intervals and modulation types. Mesh points can communicate as long as they support the same basic MCS (as well as non-11n basic rates). The selected rates apply to associated client traffic within this mesh point only.
custom (1|11|12|18|2|24|36|48|5.5|54|6|9|basic-1|basic-11|basic-12|basic-18|basic-2|basic-24|basic-36|basic-48|basic-5.5|basic-54|basic-6|basic-9|mcs0-15|mcs0-7|mcs8-15|basic-mcs0-7)	Configures custom rates • 1 – Configures the available rate at 1 Mbps • 2 – Configures the available rate at 2 Mbps • 5.5 – Configures the available rate at 5.5 Mbps • 6 – Configures the available rate at 6 Mbps • 9 – Configures the available rate at 9 Mbps • 11 – Configures the available rate at 11 Mbps • 12 – Configures the available rate at 12 Mbps • 18 – Configures the available rate at 18 Mbps • 24 – Configures the available rate at 24 Mbps • 36 – Configures the available rate at 36 Mbps • 48 – Configures the available rate at 48 Mbps • 54 – Configures the available rate at 54 Mbps • basic-1 – Configures the available rate at a basic rate of 1 Mbps • basic-2 – Configures the available rate at a basic rate of 2 Mbps • basic-5.5 – Configures the available rate at a basic rate of 5.5 Mbps • basic-6 – Configures the available rate at a basic rate of 6 Mbps • basic-9 – Configures the available rate at a basic rate of 9 Mbps • basic-11 – Configures the available rate at a basic rate of 11 Mbps • basic-12 – Configures the available rate at a basic rate of 12 Mbps • basic-18 – Configures the available rate at a basic rate of 18 Mbps • basic-24 – Configures the available rate at a basic rate of 24 Mbps • basic-36 – Configures the available rate at a basic rate of 36 Mbps • basic-48 – Configures the available rate at a basic rate of 48 Mbps • basic-54 – Configures the available rate at a basic rate of 54 Mbps • basic-mcs0-7 – Configures the MCS index range of 0 - 7 for basic rate • mcs0-7 – Configures the MCS index range of 0-7 as the data rate • mcs0-15 – Configures the MCS index range of 0-15 as the data rate • msc8-15 – Configures the MCS index range of 8-15 as the data rate Multiple choices can be made from the above list of rates

```
data-rates 5GHz [a-only|an|default]
```

data-rates 5GHz	Configures the preset data rates for the 5.0 GHz frequency
a-only	Configures the data rate for the meshpoint using 802.11a only rates
bn	Configures the data rate for the meshpoint using 802.11a and 802.11n rates
default	Configures the data rate for the meshpoint at a pre-configured default rate for this frequency
g-only	Configures the data rate for the meshpoint using 802.11g only rates
gn	Configures the data rate for the meshpoint using 802.11g and 802.11n rates

```
data-rates 5GHz custom
(12|18|24|36|48|54|6|9|basic-1|basic-11|basic-12|basic-18|
basic-2|basic-24|basic-36|basic-48|basic-5.5|basic-54|basic-6|basic-9|mcs0-15
|mcs0-7|
mcs8-15|basic-mcs0-7)
```

data-rates 5GHz	Configures the preset data rates for the 5.0 GHz frequency Define both minimum Basic and optimal Supported rates as required for 802.11a and 802.11n rates supported by the 5.0 GHz radio band. These are the rates wireless client traffic is supported within this mesh point. If supporting 802.11n, select a supported MCS index. Set a MCS in respect to the radio's channel width and guard interval. A MCS defines (based on RF channel conditions) an optimal combination of 8 data rates, bonded channels, multiple spatial streams, different guard intervals and modulation types. Mesh points can communicate as long as they support the same basic MCS (as well as non-11n basic rates). The selected rates apply to associated client traffic within this mesh point only.
custom (12|18|24|36|48|54|6|9|basic-1|basic-11|basic-12|basic-18|basic-2|basic-24|basic-36|basic-48|basic-5.5|basic-54|basic-6|basic-9|mcs0-15|mcs0-7|mcs8-15|basic-mcs0-7)	Configures custom rates • 6 – Configures the available rate at 6 Mbps • 9 – Configures the available rate at 9 Mbps • 12 – Configures the available rate at 12 Mbps • 18 – Configures the available rate at 18 Mbps • 24 – Configures the available rate at 24 Mbps • 36 – Configures the available rate at 36 Mbps • 48 – Configures the available rate at 48 Mbps • 54 – Configures the available rate at 54 Mbps • basic-1 – Configures the available rate at a basic rate of 1 Mbps • basic-2 – Configures the available rate at a basic rate of 2 Mbps • basic-5.5 – Configures the available rate at a basic rate of 5.5 Mbps • basic-6 – Configures the available rate at a basic rate of 6 Mbps • basic-9 – Configures the available rate at a basic rate of 9 Mbps • basic-11 – Configures the available rate at a basic rate of 11 Mbps • basic-12 – Configures the available rate at a basic rate of 12 Mbps • basic-18 – Configures the available rate at a basic rate of 18 Mbps • basic-24 – Configures the available rate at a basic rate of 24 Mbps • basic-36 – Configures the available rate at a basic rate of 36 Mbps • basic-48 – Configures the available rate at a basic rate of 48 Mbps • basic-54 – Configures the available rate at a basic rate of 54 Mbps • basic-mcs0-7 – Configures the MCS index range of 0-7 for basic rate • mcs0-7 – Configures the MCS index range of 0-7 as the data rate • mcs0-15 – Configures the MCS index range of 0-15 as the data rate • msc8-15 – Configures the MCS index range of 8-15 as the data rate Multiple choices can be made from the above list of rates.

Example

```
rfs7000-37FABE(config-meshpoint-test)#data-rates 2.4GHz bgn

rfs7000-37FABE(config-meshpoint-test)#data-rates 5GHz an

rfs7000-37FABE(config-meshpoint-test)#show context
meshpoint test
 meshid test
 beacon-format mesh-point
 control-vlan 1
 allowed-vlans 1,10-16,18-23
 data-rates 2.4GHz bgn
 data-rates 5GHz an
 security-mode none
```

```
 no root
rfs7000-37FABE(config-meshpoint-test)#
```

Related Commands:

no	Resets data rates for each frequency band for this meshpoint

description

meshpoint-config-instance

Configures a brief description for this meshpoint. Use this command to describe this meshpoint and its features.

Supported in the following platforms:

- Access Points — Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Access Points (as root APs only) — Brocade Mobility 650 Access Point
- Wireless Controllers — Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
description <DESCRIPTION>
```

Parameters

```
description <DESCRIPTION>
```

description	Configures a description for this meshpoint
<DESCRIPTION>	The text describing this meshpoint

Example

```
rfs7000-37FABE(config-meshpoint-test)#description "This is an example of a
meshpoint description"

rfs7000-37FABE(config-meshpoint-test)#show context
meshpoint test
 description "This is an example of a meshpoint description"
 meshid test
 beacon-format mesh-point
 control-vlan 1
 allowed-vlans 1,10-16,18-23
 data-rates 2.4GHz bgn
 data-rates 5GHz an
 security-mode none
 no root
rfs7000-37FABE(config-meshpoint-test)#
```

Related Commands:

no	Removes the human friendly description provided for this meshpoint

meshid

meshpoint-config-instance

Configures a unique *Service Set Identifier* (SSID) for this meshpoint. This ID is used to uniquely identify this meshpoint.

Supported in the following platforms:

- Access Points — Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Access Points (as root APs only) — Brocade Mobility 650 Access Point
- Wireless Controllers — Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
meshid <MESH-SSID>
```

Parameters

```
meshid <MESH-SSID>
```

meshid	Configures a unique SSID for the meshpoint
<MESH-SSID>	The unique SSID configured for this meshpoint **NOTE:** The mesh SSID is case sensitive and should not exceed 32 characters.

Example

```
rfs7000-37FABE(config-meshpoint-test)#meshid TestingMeshPoint

rfs7000-37FABE(config-meshpoint-test)#show context
meshpoint test
 description "This is an example of a meshpoint description"
 meshid TestingMeshPoint
 beacon-format mesh-point
 control-vlan 1
 allowed-vlans 1,10-16,18-23
 data-rates 2.4GHz bgn
 data-rates 5GHz an
 security-mode none
 no root
rfs7000-37FABE(config-meshpoint-test)#
```

Related Commands:

no	Removes the SSID configured for this meshpoint

neighbor

meshpoint-config-instance

This command configures the inactivity time out value for neighboring devices. If a frame is not received from the neighbor device for the configured time, then client resources are removed.

Supported in the following platforms:

- Access Points — Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Access Points (as root APs only) — Brocade Mobility 650 Access Point
- Wireless Controllers — Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
neighbor inactivity-timeout <60-86400>
```

Parameters

```
neighbor inactivity-timeout <60-86400>
```

neighbor inactivity-timeout <60-86400>	Configures the neighbor inactivity timeout in seconds. This represents the allowed interval between frames received from a neighbor before their client privileges are revoked. • <60-86400> – Specify a value from 60 - 86400 seconds. The default is 120 seconds.

Example

```
rfs7000-37FABE(config-meshpoint-test)#neighbor inactivity-timeout 300

rfs7000-37FABE(config-meshpoint-test)#show context
meshpoint test
 description "This is an example of a meshpoint description"
 meshid TestingMeshPoint
 beacon-format mesh-point
 control-vlan 1
 allowed-vlans 1,10-16,18-23
 neighbor inactivity-timeout 300
 data-rates 2.4GHz bgn
 data-rates 5GHz an
 security-mode none
 no root
rfs7000-37FABE(config-meshpoint-test)#
```

Related Commands:

no	Removes the configured neighbor inactivity time out value for this meshpoint

no

meshpoint-config-instance

Negates meshpoint commands or resets their values to default

Supported in the following platforms:

- Access Points — Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Access Points (as root APs only) — Brocade Mobility 650 Access Point
- Wireless Controllers — Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no
[allowed-vlans|beacon-format|control-vlan|description|meshid|root|security-mo
de|
          shutdown]

no data-rates [2.4GHz|5GHz]
no neighbor inactivity-timeout
no use meshpoint-qos-policy

no wpa2 [key-rotation|psk]
no wpa2 key-rotation [broadcast|unicast]
no wpa2 psk

no service allow-ht-only
```

Parameters

```
no
[allowed-vlans|beacon-format|control-vlan|description|meshid|root|security-mo
de|
shutdown]
```

no allowed-vlans	Removes all VLANs from the allowed VLANs list
no beacon-format	Resets the beacon format on this meshpoint to its default of meshpoint
no control-vlan	Removes the configured control VLAN
no description	Removes the defined description for this meshpoint
no meshid	Removes the configured mesh id for this meshpoint
no root	Removes the configuration of this meshpoint as a root meshpoint
no security-mode	Removes the configuration of security mode to use on this meshpoint to its default of “none”
no shutdown	Enables the use of this meshpoint

```
no data-rates [2.4GHz|5GHz]
```

no data-rates	Resets data rate configuration to its default
2.4GHz	Resets data rate configuration for the 2.4 GHz radio
5GHz	Resets data rate configuration for the 5.0 GHz radio

```
no neighbor inactivity-timeout
```

no neighbor	Resets the neighbor related configuration
inactivity-timeout	Resets the inactivity timeout to its default

```
no use meshpoint-qos-policy
```

no use meshpoint-qos-policy	Resets the mesh-qos-policy to default mesh-qos-policy

```
no wpa2 key-rotation [broadcast|unicast]
```

no wpa2 key-rotation	Resets the WPA2 encryption key rotation configuration for this meshpoint
broadcast	Resets the WPA2 key rotation configured for broadcast packets to its default
unicast	Resets the WPA2 key rotation configured for unicast packets to its default

```
no wpa2 psk
```

no wpq2 psk	Removes the pre shared key configured for the meshpoint

Example

```
rfs7000-37FABE(config-meshpoint-test)#show context
meshpoint test
 description "This is an example of a meshpoint description"
 meshid TestingMeshPoint
 shutdown
 beacon-format mesh-point
 control-vlan 1
 allowed-vlans 1,10-16,18-23
 neighbor inactivity-timeout 300
 data-rates 2.4GHz bgn
 data-rates 5GHz an
 security-mode psk
 wpa2 psk 0 MotorolaSolutions
 wpa2 key-rotation unicast 1200
 wpa2 key-rotation broadcast 600
 root
rfs7000-37FABE(config-meshpoint-test)#

rfs7000-37FABE(config-meshpoint-test)#no allowed-vlans
rfs7000-37FABE(config-meshpoint-test)#no beacon-format
rfs7000-37FABE(config-meshpoint-test)#no control-vlan
rfs7000-37FABE(config-meshpoint-test)#no description
rfs7000-37FABE(config-meshpoint-test)#no meshid
rfs7000-37FABE(config-meshpoint-test)#no root
rfs7000-37FABE(config-meshpoint-test)#no security-mode

rfs7000-37FABE(config-meshpoint-test)#show context
meshpoint test
 beacon-format mesh-point
 control-vlan 1
 neighbor inactivity-timeout 300
 data-rates 2.4GHz bgn
 data-rates 5GHz an
 security-mode none
 wpa2 psk 0 MotorolaSolutions
 wpa2 key-rotation unicast 1200
 wpa2 key-rotation broadcast 600
 no root

rfs7000-37FABE(config-meshpoint-test)#no data-rates 2.4GHz
rfs7000-37FABE(config-meshpoint-test)#no data-rates 5GHz

rfs7000-37FABE(config-meshpoint-test)#show context
meshpoint test
 beacon-format mesh-point
 control-vlan 1
 neighbor inactivity-timeout 300
 security-mode none
 wpa2 psk 0 MotorolaSolutions
 wpa2 key-rotation unicast 1200
 wpa2 key-rotation broadcast 600
 no root
rfs7000-37FABE(config-meshpoint-test)#
```

Related Commands:

allowed-vlans	Configures the VLANs allowed on the meshpoint
beacon-format	Configures the beacon format for the meshpoint AP
control-vlan	Configures the VLAN on which meshpoint control traffic traverses
data-rates	Configures the data rates supported per frequency band
description	Configures a human friendly description for this meshpoint
meshid	Configures a unique ID for this meshpoint
neighbor	Configures the neighbor inactivity time out for this meshpoint
root	Configures a meshpoint as the root meshpoint
security-mode	Configures the security mode to use on the meshpoint
service	Allows only 802.11n capable neighbors to create a mesh connection
shutdown	Shuts down the meshpoint
use	Configures using a QoS policy along with this meshpoint
wpa2	Configures WPA2 encryption settings

root

meshpoint-config-instance

Configures this meshpoint as the root meshpoint. Root meshpoints are generally tied to an Ethernet backhaul for wired connectivity.

Supported in the following platforms:

- Access Points — Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Access Points (as root APs only) — Brocade Mobility 650 Access Point
- Wireless Controllers — Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
root
```

Parameters

```
root
```

root {auto-mint}	Configures this meshpoint as the root meshpoint

Example

```
rfs7000-37FABE(config-meshpoint-test)#root

rfs7000-37FABE(config-meshpoint-test)#show context
meshpoint test
 description "This is an example of a meshpoint description"
 meshid TestingMeshPoint
 beacon-format mesh-point
 control-vlan 1
```

```
 allowed-vlans 1,10-16,18-23
 neighbor inactivity-timeout 300
 data-rates 2.4GHz bgn
 data-rates 5GHz an
 security-mode none
 root
rfs7000-37FABE(config-meshpoint-test)#
```

Related Commands:

no	Removes the configuration of this meshpoint as a root meshpoint

security-mode

meshpoint-config-instance

Configures the security mode for this meshpoint

Supported in the following platforms:

- Access Points — Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Access Points (as root APs only) — Brocade Mobility 650 Access Point
- Wireless Controllers — Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
security-mode [none|psk]
```

Parameters

```
security-mode [none|psk]
```

security-mode	Configures the security mode for this meshpoint
none	No security is configured for this meshpoint
psk	Uses *Pre Shared Key* (PSK) as the security mode. When using this option, use the *wpa2* command to enter a 64 character HEX or an 8-63 ASCII character passphrase used for authentication on the mesh point.

Example

```
rfs7000-37FABE(config-meshpoint-test)#security-mode psk

rfs7000-37FABE(config-meshpoint-test)#show context
meshpoint test
 description "This is an example of a meshpoint description"
 meshid TestingMeshPoint
 beacon-format mesh-point
 control-vlan 1
 allowed-vlans 1,10-16,18-23
 neighbor inactivity-timeout 300
 data-rates 2.4GHz bgn
 data-rates 5GHz an
 security-mode psk
 root
rfs7000-37FABE(config-meshpoint-test)#
```

Related Commands:

no	Resets the security configuration for this meshpoint to “none”. This indicates that no security is configured for this meshpoint.

service

meshpoint-config-instance

Use this command to allow only those neighbors who are capable of 802.11n data rates to associate with this meshpoint.

Supported in the following platforms:

- Access Points — Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Access Points (as root APs only) — Brocade Mobility 650 Access Point
- Wireless Controllers — Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
service [allow-ht-only|show cli]
```

Parameters

```
service [allow-ht-only|show cli]
```

service allow-ht-only	Allows only those neighbors who are capable of high throughput data rates (802.11n data rates) to associate with the meshpoint
service show cli	Displays running system configuration

Example

```
rfs7000-37FABE(config-meshpoint-test)#service allow-ht-only

rfs7000-37FABE(config-meshpoint-test)#show context
meshpoint test
 description "This is an example of a meshpoint description"
 meshid TestingMeshPoint
 shutdown
 beacon-format mesh-point
 control-vlan 1
 allowed-vlans 1,10-16,18-23
 neighbor inactivity-timeout 300
 data-rates 2.4GHz bgn
 data-rates 5GHz an
 security-mode psk
 wpa2 psk 0 MotorolaSolutions
 wpa2 key-rotation unicast 1200
 wpa2 key-rotation broadcast 600
 root
 service allow-ht-only
rfs7000-37FABE(config-meshpoint-test)#
```

Related Commands:

no	Resets the restriction that only 802.11n capable neighbor devices can associate with this meshpoint
service	Invokes service commands to troubleshoot or debug

shutdown

meshpoint-config-instance

Shuts down this meshpoint. Use this command to prevent an AP from participating in a mesh network.

Supported in the following platforms:

- Access Points — Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Access Points (as root APs only) — Brocade Mobility 650 Access Point
- Wireless Controllers — Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
shutdown
```

Parameters

None

Example

```
rfs7000-37FABE(config-meshpoint-test)#shutdown
rfs7000-37FABE(config)
```

Related Commands:

no	Enables an AP as a meshpoint

use

meshpoint-config-instance

Uses a *Quality of Service* (QoS) policy defined specifically for meshpoints. To use this QoS policy, it must be defined. To define a meshpoint QoS policy, see *meshpoint-qos-policy-config-instance*.

Supported in the following platforms:

- Access Points — Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Access Points (as root APs only) — Brocade Mobility 650 Access Point
- Wireless Controllers — Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
use meshpoint-qos-policy <MESHPOINT-QOS-POLICY-NAME>
```

Parameters

```
use meshpoint-qos-policy <MESHPOINT-QOS-POLICY-NAME>
```

use meshpoint-qos-poicy	Configures this meshpoint to use a predefined meshpoint QoS policy
<MESHPOINT-QOS-POLICY-NAME>	Defines the meshpoint QoS policy to use with this meshpoint

Example

```
rfs7000-37FABE(config-meshpoint-test)#use meshpoint-qos-policy test

rfs7000-37FABE(config-meshpoint-test)#show context
meshpoint test
 description "This is an example of a meshpoint description"
 meshid TestingMeshPoint
 shutdown
 beacon-format mesh-point
 control-vlan 1
 allowed-vlans 1,10-16,18-23
 neighbor inactivity-timeout 300
 data-rates 2.4GHz bgn
 data-rates 5GHz an
 security-mode psk
 root
 use meshpoint-qos-policy test
rfs7000-37FABE(config-meshpoint-test)#
```

Related Commands:

no	Removes the meshpoint QoS policy associated with this meshpoint
meshpoint-qos-policy-config-instance	Creates and configures a meshpoint QoS policy

wpa2

meshpoint-config-instance

This command sets the pre-shared keys and key rotation duration

Supported in the following platforms:

- Access Points — Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Access Points (as root APs only) — Brocade Mobility 650 Access Point
- Wireless Controllers — Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
wpa2 [psk|key-rotation]

wpa2 key-rotation [broadcast|unicast] <30-86400>
wpa2 psk [0 <SECRET>|2 <SECRET>|<SECRET>]
```

Parameters

```
wpa2 key-rotation [broadcast|unicast] <30-86400>
```

wpa2 key-rotation	Configures WPA2 key rotation settings
broadcast	Configures key rotation interval for broadcast packets When enabled, the key indices used for encrypting/decrypting broadcast traffic is alternatively rotated based on the defined interval. Key rotation enhances the broadcast traffic security on the WLAN.
unicast	Configures key rotation interval for unicast packets
<30-86400>	Configures key rotation interval from 30 - 86400 seconds for unicast or broadcast transmission

```
wpa2 psk [0 <SECRET>|2 <SECRET>|<SECRET>]
```

wpa2 psk	Configures the PSK used by this meshpoint
secret [0 <SECRET>| 2 <SECRET>|<SECRET>]	Configures the PSK used to authenticate this meshpoint with other meshpoints in the network • 0 <SECRET> – Configures a clear text secret • 2 <SECRET> – Configures an encrypted secret • <SECRET> – Specify the secret key. The shared key should not exceed 127 characters.

Example

```
rfs7000-37FABE(config-meshpoint-test)#wpa2 key-rotation broadcast 600
rfs7000-37FABE(config-meshpoint-test)#wpa2 key-rotation unicast 1200
rfs7000-37FABE(config-meshpoint-test)#wpa2 psk MotorolaSolutions

rfs7000-37FABE(config-meshpoint-test)#show context
meshpoint test
 description "This is an example of a meshpoint description"
 meshid TestingMeshPoint
 shutdown
 beacon-format mesh-point
 control-vlan 1
 allowed-vlans 1,10-16,18-23
 neighbor inactivity-timeout 300
 data-rates 2.4GHz bgn
 data-rates 5GHz an
 security-mode psk
 wpa2 psk 0 MotorolaSolutions
 wpa2 key-rotation unicast 1200
 wpa2 key-rotation broadcast 600
 root
rfs7000-37FABE(config-meshpoint-test)#
```

Related Commands:

no	Resets PSK configuration and key rotation duration

meshpoint-qos-policy-config-instance

MESHPOINT

Mesh *Quality of Service* (QoS) provides a data traffic prioritization scheme. QoS reduces congestion from excessive traffic. If there is enough bandwidth for all users and applications (unlikely because excessive bandwidth comes at a very high cost), then applying QoS has very little value. QoS provides policy enforcement for mission-critical applications and/or users that have critical bandwidth requirements when bandwidth is shared by different users and applications.

Mesh QoS helps ensure each mesh point on the mesh network receives a fair share of the overall bandwidth, either equally or as per the proportion configured. Packets directed towards clients are classified into categories such as video, voice and data.packets within each category are processed based on the weights defined for each mesh point.

To create a meshpoint, see *meshpoint-config-instance*. A meshpoint QoS policy is created from the (config) instance. To create a meshpoint QoS policy use the following command:

```
<DEVICE>(config)#meshpoint-qos-policy <POLICYNAME>

rfs7000-37FABE(config)#meshpoint-qos-policy test
rfs7000-37FABE(config-meshpoint-qos-test)#

rfs7000-37FABE(config-meshpoint-qos-test)#?
Mesh Point QoS Mode commands:
  accelerated-multicast  Configure accelerated multicast streams address and
                         forwarding QoS classification
  no                     Negate a command or set its defaults
  rate-limit             Configure traffic rate-limiting parameters on a
                         per-meshpoint/per-neighbor basis

  clrscr                 Clears the display screen
  commit                 Commit all changes made in this session
  do                     Run commands from Exec mode
  end                    End current mode and change to EXEC mode
  exit                   End current mode and down to previous mode
  help                   Description of the interactive help system
  revert                 Revert changes
  service                Service Commands
  show                   Show running system information
  write                  Write running configuration to memory or terminal

rfs7000-37FABE(config-meshpoint-qos-test)#
```

The following table summarizes the mespoint-qos-policy configuration commands.

Command	Description	Reference
accelerated-multicast	Configures accelerated multicast parameters	page 1285
no	Negates a command or reverts settings to their default	page 1286
rate-limit	Configures the rate limits for this QoS policy	page 1287
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

accelerated-multicast

meshpoint-qos-policy-config-instance

Configures the accelerated multicast stream's address and forwarding QoS classification

NOTE
For accelerated multicast feature to work, IGMP querier must be enabled.

When a user joins a multicast stream, an entry is created in the device's (AP or wireless controller) snoop table and the entry is set to expire after a set time period. Multicast packets are forwarded to the appropriate wireless LAN or mesh until this entry is available in the snoop table.

Snoop querier keeps the snoop table current by updating entries that are set to expire. It also keeps an entry for each multicast stream till there are users registered for the stream.

Supported in the following platforms:

- Access Points — Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Access Points (as root APs only) — Brocade Mobility 650 Access Point
- Wireless Controllers — Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
accelerated-multicast [<MULTICAST-IP>|autodetect] {classification
[background|
          best-effort|trust|video|voice]}
```

Parameters

```
accelerated-multicast [<MULTICAST-IP>|autodetect] {classification
[background|
best-effort|trust|video|voice]}
```

accelerated-multicast	Configures the accelerated multicast stream address and forwarding QoS classification
<MULTICAST-IP>	Specify a list of multicast addresses and classifications. Packets are accelerated when the destination address matches.
autodetect	Lets the system to automatically detect multicast streams to be accelerated This option allows the administrator to convert multicast packets to unicast in order to provide better overall airtime utilization and performance. The system can be configured to automatically detect multicast streams and convert them to unicast, or specify which multicast streams are to be converted to unicast. When the stream is converted and being queued up for transmission, there are a number of classification mechanisms applied to the stream and the administrator can select what type of classification they would want. Classification types are trust, voice, video, best effort, and background.
classification	Optional. Defines the QoS classification to apply to a multicast stream. The following options are available: • background • best effort • trust • video • voice

Example

```
rfs7000-37FABE(config-meshpoint-qos-test)#accelerated-multicast 224.0.0.1
classification video

rfs7000-37FABE(config-meshpoint-qos-test)#show context
meshpoint-qos-policy test
 accelerated-multicast 224.0.0.1 classification video
rfs7000-37FABE(config-meshpoint-qos-test)#
```

Related Commands:

no	Resets accelerated multicast configurations for this meshpoint QoS policy

no

meshpoint-qos-policy-config-instance

Negates the commands for meshpoint QoS policy or resets their values to their default

Supported in the following platforms:

- Access Points — Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Access Points (as root APs only) — Brocade Mobility 650 Access Point
- Wireless Controllers — Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
no [accelerated-multicast|rate-limit]

no accelerated-multicast [<MULTICAST-IP>|autodetect]
rate-limit [meshpoint|neighbor] [from-air|to-air] {max-burst-size|rate}
no rate-limit [meshpoint|neighbor] [from-air|to-air] {red-threshold
[background|
          best-effort|video|voice]}
```

Parameters

```
no accelerated-multicast [<MULTICAST-IP>|autodetect]
```

accelerated-multicast	Resets the accelerated multicast stream address and forwarding QoS classification
<MULTICAST-IP>	Defines the IP address of the multicast stream to be reset
autodetect	Lets the system automatically detect multicast streams to be reset

```
no rate-limit [meshpoint|neighbor] [from-air|to-air] {max-burst-size|rate}
```

meshpoint	Resets rate limit parameters for a meshpoint
neighbor	Resets rate limit parameters for neighboring meshpoint devices
from-air	Resets rate limit value for traffic from the wireless neighbor to the network.
to-air	Resets the rate limit value for traffic from the network to the wireless neighbor.
max-burst-size	Optional. Resets the maximum burst size in kilobytes
rate	Optional. Configures the maximum traffic rate in kilobytes.

```
no rate-limit [meshpoint|neighbor] [from-air|to-air] {red-threshold
[background|
best-effort|video|voice]}
```

meshpoint	Resets rate limit parameters for a meshpoint
neighbor	Resets rate limit parameters for neighboring meshpoint devices
from-air	Resets the rate limit value for traffic from the wireless neighbor to the network
to-air	Resets the rate limit value for traffic from the network to the wireless neighbor
red-threshold	Optional. Resets the *random early detection* (RED) threshold for traffic class. The options are: • background – Resets the threshold for low priority traffic • best-effort – Resets the threshold for best effort traffic • video – Resets the threshold for video traffic • voice – Resets the threshold for voice traffic

Example

```
rfs7000-37FABE(config-meshpoint-qos-test)#show context
meshpoint-qos-policy test
 rate-limit meshpoint from-air rate 80000
 rate-limit meshpoint from-air red-threshold video 80
 rate-limit meshpoint from-air red-threshold voice 70
 accelerated-multicast 224.0.0.1 classification video

rfs7000-37FABE(config-meshpoint-qos-test)#no rate-limit meshpoint from-air
rate
rfs7000-37FABE(config-meshpoint-qos-test)#no rate-limit meshpoint from-air
red-threshold video 80
rfs7000-37FABE(config-meshpoint-qos-test)#no rate-limit meshpoint from-air
red-threshold voice 70

rfs7000-37FABE(config-meshpoint-qos-test)#show context
meshpoint-qos-policy test
 accelerated-multicast 224.0.0.1 classification video
rfs7000-37FABE(config-meshpoint-qos-test)#
```

rate-limit

meshpoint-qos-policy-config-instance

Configures the rate limiting of traffic on a per meshpoint or per neighbor basis

Excessive traffic can cause performance issues or bring down the network entirely. Excessive traffic, bombardments and interference are caused by numerous sources, such as network loops, faulty devices, or malicious software (such as a worm or virus) that has infected one or more branch-level devices. Rate limiting limits the maximum rate sent to or received from the wireless network (and meshpoint) per neighbor. It prevents any single user from overwhelming the wireless network. It also provides differential service for service providers. An administrator can set separate QoS rate limit configurations for data transmitted from the network and data transmitted from a mesh point's neighbor.

Before defining rate limit thresholds for meshpoint transmit and receive traffic, Brocade recommends you define the normal number of ARP, broadcast, multicast, and unknown unicast packets that typically transmit and receive from each supported WMM access category. If thresholds are defined too low, normal network traffic (required by end-user devices) is dropped, resulting in intermittent outages and performance problems.

A connected neighbor can also have QoS rate limit settings defined in both the transmit and receive direction.

Supported in the following platforms:

- Access Points — Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Access Points (as root APs only) — Brocade Mobility 650 Access Point
- Wireless Controllers — Brocade Mobility RFS6000, Brocade Mobility RFS7000
- Service Platforms — Brocade Mobility RFS9510

Syntax:

```
rate-limit [meshpoint|neighbor]

rate-limit [meshpoint|neighbor] [from-air|to-air] {max-burst-size <2-1024>|
          rate <50-1000000>}
rate-limit [meshpoint|neighbor] [from-air|to-air] {red-threshold [background
<0-100>|
          best-effort <0-100>|video <0-100>|voice <0-100>]}
```

Parameters

```
rate-limit [meshpoint|neighbor] [from-air|to-air] {max-burst-size <2-1024>|
rate <50-1000000>}
```

meshpoint	Configures rate limit parameters for all data received from any meshpoint in the mesh network. This option is disabled by default.
neighbor	Configures rate limit parameters for neighboring meshpoint devices. Enables rate limiting for data transmitted from the client to its associated access point radio and connected controller. This option is disabled by default.
from-air	Configures rate limits for traffic from the wireless neighbor to the network.
to-air	Configures rate limits for traffic from the network to the wireless neighbor.
max-burst-size <2-1024>	Optional. Configures the maximum burst size in kilobytes. Set a value from 2 - 1024 kbytes. For a meshpoint: The smaller the burst, the less likely that the transmit packet transmission results in congestion for the meshpoint's client destinations. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should then add a 10% margin (minimally) to allow for traffic bursts at the site. The default burst size is 320 kbytes. For a neighbor: The smaller the burst, the less likely the transmit packet transmission will result in congestion for the wireless client. The default burst size is 64 kbytes.
rate <50-1000000>	Optional. Defines a receive or transmit rate limit in kilobytes per second. Set a value from 50 - 1000000 kbps. For a meshpoint: This limit constitutes a threshold for the maximum the number of packets transmitted or received over the meshpoint (from all access categories). Traffic that exceeds the defined rate is dropped and a log message is generated. The default setting is 5000 kbps. For a neighbor: This limit constitutes a threshold for the maximum the number of packets transmitted or received (from all access categories). Traffic that exceeds the defined rate is dropped by the client and a log message is generated. The default rate is 1,000 kbps.

```
rate-limit [meshpoint|neighbor] [from-air|to-air]
{red-threshold [background <0-100>|best-effort <0-100>|video <0-100>|voice
<0-100>]}
```

meshpoint	Configures rate limit parameters for a meshpoint
neighbor	Configures rate limit parameters for neighboring meshpoint devices
from-air	Configures rate limits for traffic from the wireless neighbor to the network
to-air	Configures rate limit value for traffic from the network to the wireless neighbor
red-threshold	Optional. Configures *random early detection* threshold (RED threshold) for traffic class
background <0-100>	The following keyword is applicable to the 'from-air' and 'to-air' traffics. Configures the threshold for low priority (background) traffic For a meshpoint: This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped and a log message is generated. Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general transmit rate is known by the network administrator (using a time trend analysis). The default threshold is 50%. For a neighbor: This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default threshold is 50%.
best-effort <0-100>	The following keyword is applicable to the 'from-air' and 'to-air' traffics. Configures the threshold for best effort traffic For a meshpoint: This is a percentage of the maximum burst size for normal priority traffic. Best effort traffic exceeding the defined threshold is dropped and a log message is generated. Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general transmit rate is known by the network administrator (using a time trend analysis). The default threshold is 50%. For a neighbor: This is a percentage of the maximum burst size for normal traffic. Best effort traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default threshold is 50%.
video <0-100>	The following keyword is applicable to the 'from-air' and 'to-air' traffics. Configures the threshold for video traffic For a meshpoint: This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped and a log message is generated. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general transmit rate is known by the network administrator (using a time trend analysis). The default threshold is 25%. For a neighbor: This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default threshold is 25%.
voice <0-100>	The following keyword is applicable to the 'from-air' and 'to-air' traffics. Configures the threshold for voice traffic For a meshpoint: This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped and a log message is generated. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 0%. For a neighbor: This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default threshold is 0% and implies no early random drops will occur.

Example

```
rfs7000-37FABE(config-meshpoint-qos-test)#rate-limit meshpoint from-air
max-burst-size 800

rfs7000-37FABE(config-meshpoint-qos-test)#show context
meshpoint-qos-policy test
 rate-limit meshpoint from-air max-burst-size 800
```

```
 accelerated-multicast 224.0.0.1 classification video

rfs7000-37FABE(config-meshpoint-qos-test)#rate-limit meshpoint from-air rate
80000

rfs7000-37FABE(config-meshpoint-qos-test)#rate-limit meshpoint from-air
red-threshold video 80

rfs7000-37FABE(config-meshpoint-qos-test)#rate-limit meshpoint from-air
red-threshold voice 70

rfs7000-37FABE(config-meshpoint-qos-test)#show context
meshpoint-qos-policy test
 rate-limit meshpoint from-air rate 80000
 rate-limit meshpoint from-air max-burst-size 800
 rate-limit meshpoint from-air red-threshold video 80
 rate-limit meshpoint from-air red-threshold voice 70
 accelerated-multicast 224.0.0.1 classification video
rfs7000-37FABE(config-meshpoint-qos-test)#
```

Related Commands:

no	Resets traffic rate limit settings for this meshpoint QoS policy

meshpoint-device-config-instance

MESHPOINT

The following table lists the meshpoint device configuration commands.

Command	Description	Reference
meshpoint-device	Configures an access point as a meshpoint device and enters its configuration mode	page 1290
meshpoint-device-commands	Invokes the meshpoint-device configuration commands	page 1292

meshpoint-device

meshpoint-device-config-instance

This command configures an access point to use a defined meshpoint. This command is available only under the Brocade Mobility 650 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point device or profile context. To configure this feature use one of the following options:

- navigate to the device profile config context (used when configuring access point profile on a controller)
- navigate to the device's config context using the self command (used when configuring a logged on access point)

Supported in the following platforms:

- Access Points — Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Access Points (as root APs only) — Brocade Mobility 650 Access Point

Syntax:

```
meshpoint-device <MESHPOINT-NAME>
```

Parameters

```
meshpoint-device <MESHPOINT-NAME>
```

meshpoint-device	Configures the AP as a meshpoint device and sets its parameters
<MESHPOINT-NAME>	The meshpoint to configure the AP with

Example

```
rfs7000-37FABE(config)#profile br71xx AP71XXTestProfile
rfs7000-37FABE(config-profile-AP71XXTestProfile)#meshpoint-device test
rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#

rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#?
Mesh Point Device Mode commands:
  Mesh Point Device Mode commands:
  acs          Configure auto channel selection parameters
  exclude      Exclude neighboring Mesh Devices
  hysteresis   Configure path selection SNR hysteresis values
  monitor      Event Monitoring
  no           Negate a command or set its defaults
  path-method  Path selection method used to find a root node
  preferred    Configure preferred path parameters
  root         Set this meshpoint as root

  clrscr       Clears the display screen
  commit       Commit all changes made in this session
  do           Run commands from Exec mode
  end          End current mode and change to EXEC mode
  exit         End current mode and down to previous mode
  help         Description of the interactive help system
  revert       Revert changes
  service      Service Commands
  show         Show running system information
  write        Write running configuration to memory or terminal

rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#

br7131-139B34(config-device-00-23-68-13-9B-34)#meshpoint-device test
br7131-139B34(config-device-00-23-68-13-9B-34-meshpoint-test)#?
Mesh Point Device Mode commands:
  acs          Configure auto channel selection parameters
  exclude      Exclude neighboring Mesh Devices
  hysteresis   Configure path selection SNR hysteresis values
  monitor      Event Monitoring
  no           Negate a command or set its defaults
  path-method  Path selection method used to find a root node
  preferred    Configure preferred path parameters
  root         Set this meshpoint as root

  clrscr       Clears the display screen
  commit       Commit all changes made in this session
  do           Run commands from Exec mode
  end          End current mode and change to EXEC mode
  exit         End current mode and down to previous mode
  help         Description of the interactive help system
```

```
  revert       Revert changes
  service      Service Commands
  show         Show running system information
  write        Write running configuration to memory or terminal

br7131-139B34(config-device-00-23-68-13-9B-34-meshpoint-test)#?
```

meshpoint-device-commands

meshpoint-device-config-instance

The following table lists the meshpoint-device configuration mode commands

Command	Description	Reference
acs	Enables *Automatic Channel Selection* (ACS) on this meshpoint device (access point)	page 1292
exclude	Excludes neighboring mesh devices	page 1296
hysteresis	Configures path selection SNR hysteresis values on this meshpoint-device (access point)	page 1297
monitor	Enables monitoring of critical resource and primary port links on a meshpoint device	page 1298
path-method	Configures the method used to select the path to the root node in a mesh network	page 1298
preferred	Configures the preferred path parameters for a meshpoint device	page 1299
root	Configures a meshpoint device as the root meshpoint	page 1300
root-select	Configures this meshpoint device as the cost root	page 1301
no	Negates the commands for a meshpoint device or resets values to default	page 1302

acs

meshpoint-device-commands

Enables *Automatic Channel Selection* (ACS) on this meshpoint device (access point). When enabled, this feature automatically selects the best channel for a meshpoint-device radio based on the device configuration, channel conditions, and network layout.

In a wireless network deployment, it is advantageous for network devices to have the ability to operate in multiple channels and not be limited to only a single channel. Multiple channels increase the bandwidth and throughput of the wireless network. In such a scenario, each network device must have a mechanism to dynamically select a suitable channel of operation. ACS provides the required mechanism for a MCX enabled device.

Use this command to configure the ACS settings and override the default meshpoint configurations.

Supported in the following platforms:

- Access Points — Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Access Points (as root APs only) — Brocade Mobility 650 Access Point

Syntax:

```
acs
[channel-hold-time|channel-switch-delta|channel-width|ocs-duration|ocs-freque
ncy|

path-min|path-threshold|priority-meshpoint|sample-count|snr-delta|signal-thre
shold|
          tolerance-period]

acs channel-hold-time [2.4GHz|5GHz] <0-86400>

acs channel-switch-delta [2.4GHz|5GHz] <5-35>

acs channel-width [2.4GHz|5GHz] [20MHz|40MHz|auto]

acs ocs-duration [2.4GHz|5GHz] <20-250>

acs ocs-frequency [2.4GHz|5GHz] <1-60>

acs path-min [2.4GHz|5GHz] <100-20000>

acs path-threshold [2.4GHz|5GHz] <800-65535>

acs priority-meshpoint [2.4GHz|5GHz] <MESHPOINT-NAME>

acs sample-count [2.4GHz|5GHz] <1-10>

acs snr-delta [2.4GHz|5GHz] <1-100>

acs signal-threshold [2.4GHz|5GHz] <-100-0>

acs tolerance-period [2.4GHz|5GHz] <10-600>
```

Parameters

```
acs channel-hold-time [2.4GHz|5GHz] <0-86400>
```

acs	Configures ACS settings and overrides on the selected meshpoint-device
channel-hold-time [2.4GHz|5GHz] <0-86400>	Configures the minimum time, in seconds, before a periodic scan, to assess channel conditions for a meshpoint root, is triggered. • 2.4 GHz – Configures the channel hold interval for the 2.4 GHz radio band • 5.0GHz – Configures the channel hold interval for the 5.0 GHz radio band The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands: • <0-86400> – Specify a value from 0 - 86400 seconds. The default is 1800 seconds. A value of '0' disables periodic channel assessment.

```
acs channel-switch-delta [2.4GHz|5GHz] <5-35>
```

acs	Configures ACS settings and overrides on the selected meshpoint-device
channel-switch-delta [2.4GHz|5GHz] <5-35>	Configures the difference in interference between the current and best channel needed to trigger a channel change. Once the difference in the current channel and the best channel interference equals the configured value, a channel change is triggered. • 2.4 GHz – Configures the channel switch delta for the 2.4GHz radio band • 5.0GHz – Configures the channel switch delta for the 5.0 GHz radio band The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands: • <5-35> – Specify a value from 5 - 35 dBm. The default is 10 dBm.

`acs channel-width [2.4GHz|5GHz] [20MHz|40MHz|auto]`

acs	Configures ACS settings and overrides on the selected meshpoint-device
channel-width [2.4GHz|5GHz] [20MHz|40MHz|auto]	Configures the channel width that meshpoint auto channel selection assigns to the radio • 2.4 GHz – Configures the operating channel width for the 2.4 GHz radio band • 5.0 GHz – Configures the operating channel width for the 5.0 GHz radio band The following keywords are common to the '2.4 GHz' and '5.0 GHz' bands: • 20 MHz – Assigns the 20 MHz channel width to the radio • 40 MHz – Assigns the 40 MHz channel width to the radio • auto – Selects and assigns the best possible channel from the 20/40 MHz width. This is the default setting.

`acs ocs-duration [2.4GHz|5GHz] <20-250>`

acs	Configures ACS settings and overrides on the selected meshpoint-device
ocs-duration [2.4GHz|5GHz] <20-250>	Configures the duration, in milliseconds, of *off -channel scans* (OCSs) • 2.4 GHz – Configures the ocs-duration for the 2.4 GHz radio band • 5.0 GHz – Configures the ocs-duration for the 5.0 GHz radio band The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands: • <20-250> – Specify a value from 20 - 250 milliseconds. The default value is 50 milliseconds.

`acs ocs-frequency [2.4GHz|5GHz] <1-60>`

acs	Configures ACS settings and overrides on the selected meshpoint-device
ocs-frequency [2.4GHz|5GHz] <1-60>	Configures the interval, in seconds, at which off-channel scan is performed. An ocs-frequency of 10 seconds means that an off-channel scan will be performed once every 10 seconds. • 2.4 GHz – Configures the ocs-frequency for the 2.4 GHz radio band • 5.0 GHz – Configures the ocs-frequency for the 5.0 GHz radio band The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands: • <1-60> – Specify a value form 1 - 60 seconds. The default is 6 seconds.

`acs path-min [2.4GHz|5GHz] <100-20000>`

acs	Configures ACS settings and overrides on the selected meshpoint-device
path-min [2.4GHz|5GHz] <100-20000>	Configures the minimum root path metric needed for auto channel selection. This is the acceptance root path metric value to consider a root as a possible candidate mesh node. • 2.4 GHz – Configures the minimum root path metric for the 2.4 GHz radio band • 5.0 GHz – Configures the minimum root path metric for the 5.0 GHz radio band The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands: • <100-20000> – Specify a value from 100 - 20000. The default is 1000.

`acs path-threshold [2.4GHz|5GHz] <800-65535>`

acs	Configures ACS settings and overrides on the selected meshpoint-device
path-threshold [2.4GHz|5GHz] <800-65535>	Configures the root path metric threshold for auto channel selection. This is the acceptance root path metric threshold beyond which the root bound to is considered as bad. • 2.4 GHz – Configures the root path metric threshold for the 2.4 GHz radio band • 5.0 GHz – Configures the root path metric threshold for the 5.0 GHz radio band The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands: • <800-65535> – Specify a value from 800 -65535. The default is 1500.

`acs priority-meshpoint [2.4GHz|5GHz] <MESHPOINT-NAME>`

acs	Configures ACS settings and overrides on the selected meshpoint-device
priority-meshpoint [2.4GHz|5GHz] <MESHPOINT-NAME>	Configures the priority meshpoint. Configuring a priority meshpoint overrides automatic meshpoint configuration. • 2.4 GHz – Configures the priority meshpoint for the 2.4 GHz radio band • 5.0 GHz – Configures the priority meshpoint for the 5.0 GHz radio band The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands: • <MESHPOINT-NAME> – Specify the meshpoint name for the selected radio band.

`acs sample-count [2.4GHz|5GHz] <1-10>`

acs	Configures ACS settings and overrides on the selected meshpoint-device
sample-count [2.4GHz|5GHz] <1-10>	Configures the minimum number of scan cycle samples to consider for auto channel selection • 2.4 GHz – Configures the sample count for the 2.4 GHz radio band • 5.0 GHz – Configures the sample count for the 5.0 GHz radio band The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands: • <1-10> – Specify a value from 1 -10. The default is 5 samples.

`acs snr-delta [2.4GHz|5GHz] <1-100>`

acs	Configures ACS settings and overrides on the selected meshpoint-device
snr-delta [2.4GHz|5GHz] <1-100>	Configures the channel SNR delta. A meshpoint on a candidate channel must have a SNR of a greater delta than the next hop on the current channel. • 2.4 GHz – Configures the snr-delta for the 2.4 GHz radio band • 5.0 GHz – Configures the snr-delta for the 5.0 GHz radio band The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands: • <1-100> – Specify a value from 1 - 100 dB. The default is 5 dB.

`acs signal-threshold [2.4GHz|5GHz] <-100-0>`

acs	Configures ACS settings and overrides on the selected meshpoint-device
signal-threshold [2.4GHz|5GHz] <-100-0>	Configures the signal strength threshold. If the signal strength of the next hop drops below the configured signal-threshold, a scan is triggered. • 2.4 GHz – Configures the signal-threshold for the 2.4 GHz radio band • 5.0 GHz – Configures the signal-threshold for the 5.0 GHz radio band The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands: • <-100-0> – Specify a value from -100 - 0 dB. The default is -65 dB.

`acs tolerance-period [2.4GHz|5GHz] <10-600>`

acs	Configures ACS settings and overrides on the selected meshpoint-device
tolerance-period [2.4GHz|5GHz] <10-600>	Configures the maximum tolerance period in seconds. This is the interval to wait for the root bound to recovery from a bad link. • 2.4 GHz – Configures the tolerance-period for the 2.4 GHz radio band • 5.0 GHz – Configures the tolerance-period for the 5.0 GHz radio band The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands: • <10-600> – Specify a value from 10 - 600 seconds. the default is 60 seconds.

Example

```
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#acs
channel-hold-time 2.4GHz 2500
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#

rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#acs ocs-duration
2.4GHz 30
```

```
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#

rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#acs ocs-frequency
2.4GHz 1
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#

rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#show context
 meshpoint-device test
  acs ocs-frequency 2.4GHz 1
  acs osc-duration 2.4GHz 30
  acs channel-hold-time 2.4GHz 2500
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#
```

Related Commands:

no	Reverts the configured ACS settings to default

exclude

meshpoint-device-commands

Enables wired-peer (that are wired MiNT level-1 neighbors) exclusion

Supported in the following platforms:

- Access Points — Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Access Points (as root APs only) — Brocade Mobility 650 Access Point

Syntax:

```
exclude wired-peer mint-level-1
```

Parameters

```
exclude wired-peer mint-level-1
```

exclude wired-peer	Excludes neighboring mesh devices
wired-peer mint-level-1	Excludes neighboring wired mesh devices with MiNTlevel-1 link When enabled, all neighboring wired mesh devices are excluded from mesh links.

Example

```
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#exclude wired-peer
mint-level-1
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#

rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#show context
 meshpoint-device test
  exclude wired-peer mint-level-1
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#
```

Related Commands:

no	Disables wired-peer exclusion on this meshpoint

hysteresis

meshpoint-device-commands

Configures path selection SNR hysteresis values on this meshpoint-device (access point). These are settings that facilitate dynamic path selection. Configuring hysteresis prevents frequent re-ranking of the shortest path cost.

Supported in the following platforms:

- Access Points — Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Access Points (as root APs only) — Brocade Mobility 650 Access Point

Syntax:

```
hysteresis [min-threshold|period|root-sel-snr-delta|snr-delta]

hysteresis [min-threshold <-100-0>|period <0-600>|root-sel-snr-delta <1-100>|
          snr-delta <1-100>]
```

Parameters

```
hysteresis [min-threshold <-100-0>|period <0-600>|root-sel-snr-delta
<1-100>|snr-delta <1-100>]
```

min-threshold <-100-0>	Configures the minimum signal strength that a device should have to be considered a likely candidate in the mesh route (to the mesh root node) selection process. • <-100-0> – Specify a value from -100 - 0 dB. The default is 0 dB.
period <0-600>	Configures the interval, in seconds, for which a likely candidate's path method hysteresis is sustained. In other words a device capable of sustaining the signal strength for the specified period of time is a likely candidate in the mesh route (to the mesh root node) selection process. • <0-600> – Specify a value from 0 - 600 seconds. The default is 1 second
root-sel-snr-delta <1-100>	Configures the signal strength, in dB, that a device has to sustain, within the delta range, to be considered a likely candidate in the mesh route (to the mesh root node) selection process. • <1-100> – Specify a value from 1 - 100 dB.
snr-delta <1-100>	Configures the SNR delta. The device with must have a SNR of a greater delta than its current neighbor to be considered a likely candidate in the mesh route (to the mesh root) selection process. • <1-100> – Specify a value from 1 - 100 dB. The default is 1 dB.

Example

```
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#hysteresis period 15

rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#hysteresis
root-sel-snr
-delta 12

rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#hysteresis snr-delta
3

rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#hysteresis
min-threshold -65

rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#show context
 meshpoint-device test
  hysteresis period 15
  hysteresis snr-delta 3
```

```
  hysteresis min-threshold -65
  hysteresis root-sel-snr-delta 12
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#
```

Related Commands:

no	Removes the configured path selection SNR hysteresis values

monitor

meshpoint-device-commands

Enables monitoring of critical resource and primary port links. It also configures the action taken in case a critical resource goes down or a primary port link is lost.

Supported in the following platforms:

- Access Points — Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Access Points (as root APs only) — Brocade Mobility 650 Access Point

Syntax:

```
monitor [critical-resource|primary-port-link-loss]
monitor [critical-resource|primary-port-link-loss] action no-root
```

Parameters

```
monitor [critical-resource|primary-port-link-loss] action no-root
```

critical-resource	Enables critical resource down event monitoring
primary-port-link-loss	Enables primary port link loss event monitoring
action	The following are common to all of the above: • action – Sets the action taken if a critical resource goes down or if a primary port link is lost • no-root – Changes the meshpoint to be non root (this is the action taken in case any of the above mentioned two events occur)

Example

```
rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#monitor
critical-resource action no-root

rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#show context
 meshpoint-device test
  name test
  monitor critical-resource action no-root
rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#
```

Related Commands:

no	Disables monitoring of critical resource and primary port links.

path-method

meshpoint-device-commands

Configures the path selection method used on a meshpoint device. This is the method used to select the route to the root node within a mesh network.

Supported in the following platforms:

- Access Points — Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Access Points (as root APs only) — Brocade Mobility 650 Access Point

Syntax:

```
path-method [mobile-snr-leaf|snr-leaf|uniform]
```

Parameters

```
path-method [mobile-snr-leaf|snr-leaf|uniform]
```

path-method	Sets the method used to select the path to the root node in a mesh network
mobile-snr-leaf	Configures the path selection method as mobile-snr-leaf. When selected, the path to the root node is selected based on the *Signal-to-Noise Ratio* (SNR) to a neighboring device. This option allows meshpoint devices to select a neighbor with the strongest SNR. Meshpoint devices using the mobile-snr-leaf method are non-forwarding nodes in the meshpoint traffic. **NOTE:** Select this option for *Vehicular Mounted Modem* (VMM) access points or other mobile devices.
snr-leaf	This option allows meshpoints to select a neighbor with the strongest SNR. It is similar to the mobile-snr-leaf option, but is not applicable to mobile devices, such as VMMs.
uniform	Indicates the path selection method is uniform. When selected, two paths will be considered equivalent if the average goodput is the same for both paths. This is the default setting. **NOTE:** Select this option for infrastructure devices.

Example

```
rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#path-method
mobile-snr-leaf
rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#

rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#show context
 meshpoint-device TEST
  name TEST
  path-method mobile-snr-leaf
rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#
```

Related Commands:

no	Resets the path selection method on a meshpoint device

preferred

meshpoint-device-commands

Configures the preferred path parameters for this meshpoint device

Supported in the following platforms:

- Access Points — Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Access Points (as root APs only) — Brocade Mobility 650 Access Point

Syntax:

```
preferred [neighbor <MAC>|root <MAC>|interface [2.4GHz|4.9GHz|5GHz]]
```

Parameters

```
preferred [neighbor <MAC>|root <MAC>|interface [2.4GHz|4.9GHz|5GHz]]
```

preferred	Configures the preferred path parameters
neighbor <MAC>	Adds the MAC address of a neighbor meshpoint as a preferred neighbor
root <MAC>	Adds the MAC address of a root meshpoint as a preferred root
interface [2.4GHz|4.9GHz|5GHz]	Sets the preferred interface

Example

```
rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#preferred
neighbor
11-22-33-44-55-66

rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#preferred
root
22-33-44-55-66-77

rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#preferred
interface 5GHz

rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#show context
 meshpoint-device test
  name test
  preferred root 22-33-44-55-66-77
  preferred neighbor 11-22-33-44-55-66
  preferred interface 5GHz
  monitor critical-resource action no-root
rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#
```

Related Commands:

no	Removes the configuration of preferred paths for this meshpoint device

root

meshpoint-device-commands

Configures this meshpoint device as the root meshpoint

You can optionally use the select-method option to enable dynamic mesh selection. When enabled, this option overrides root or no-root configuration and uses the selection method.

Supported in the following platforms:

- Access Points — Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Access Points (as root APs only) — Brocade Mobility 650 Access Point

Syntax:

```
root {select-method auto-mint}
```

Parameters

`root {select-method auto-mint}`

root	Configures this meshpoint device as the root meshpoint
select-method auto-mint	Optional. Enables or disables dynamic mesh selection. When enabled, this option overrides root or no-root configuration and chooses the selection method. • auto-mint – Enables dynamic root selection using Auto-MiNT (based on path cost) The Auto-Mint or Cost Method dynamically determines the root/non-root configuration of a meshpoint by: • Monitoring and ranking the signal strength and path cost of neighboring mesh points. • Setting the configuration to: • non-root: If the link with the shortest path to the cost-root mesh device is a MCX meshpoint link • root: If the link with the shortest path to the cost-root mesh device is a non MCX meshpoint link (wired link). This requires that the meshpoint device, in the brain car, be configured as the 'cost root' and the 'cost root' meshpoint-device be the l2 gateway to the controller. Use the *root-select > cost-root* command to configure a meshpoint-device as 'cost-root'. • Using signal strength of neighboring meshpoint as the sole metric to determine the next mesh hop to the root. • Loop detection with both meshpoints in a car select non-root and form a mesh link with the same root

Example

```
rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#root

rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#show context
 meshpoint-device test
  name test
  root
  preferred root 22-33-44-55-66-77
  preferred neighbor 11-22-33-44-55-66
  preferred interface 5GHz
  monitor critical-resource action no-root
rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#

ap7131-11E6C4(config-device-00-23-68-11-E6-C4-meshpoint-test)#root
select-method
 auto-mint

ap7131-11E6C4(config-device-00-23-68-11-E6-C4-meshpoint-test)#show context
 meshpoint-device test
  root select-method auto-mint
ap7131-11E6C4(config-device-00-23-68-11-E6-C4-meshpoint-test)#
```

Related Commands:

no	Removes the configuration of this meshpoint device as a root meshpoint. Also allows you to disable dynamic mesh selection (if enabled).

root-select

meshpoint-device-commands

Configures this meshpoint device as the cost root

Supported in the following platforms:

- Access Points — Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Access Points (as root APs only) — Brocade Mobility 650 Access Point

Syntax:

```
root-select cost-root
```

Parameters

```
root-select cost-root
```

root-select cost-root	Configures this meshpoint device as the cost root. This is necessary for dynamic root selection process.

Example

```
ap7131-11E6C4(config-device-00-23-68-11-E6-C4-meshpoint-test)#root-select
cost-root

ap7131-11E6C4(config-device-00-23-68-11-E6-C4-meshpoint-test)#show context
 meshpoint-device test
  root select-method auto-mint
  root-select cost-root
ap7131-11E6C4(config-device-00-23-68-11-E6-C4-meshpoint-test)#
```

Related Commands:

no	Removes this meshpoint-device as the cost-root

no

meshpoint-device-commands

Negates the commands for a meshpoint device or resets values to default

Supported in the following platforms:

- Access Points — Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Access Points (as root APs only) — Brocade Mobility 650 Access Point

Syntax:

```
no [acs|exclude|hysteresis|monitor|path-method|preferred|root|root-select]

no acs [channel-hold-time|channel-switch-delta|channel-width|ocs-duration|

ocs-frequency|path-min|path-threshold|priority-meshpoint|sample-count|snr-del
ta|
          signal-threshold|tolerance-period] [2.4GHZ|5GHz]

no exclude wired-peer mint-level-1

no hysteresis [min-threshold|period|root-sel-snr-delta|snr-delta]

no monitor [critical-resource|primary-port-link-loss]

no [path-method|root {select-method}]
```

```
no root-select cost-root

no preferred [interface|root|neighbor]
```

Parameters

```
no acs [channel-hold-time|channel-switch-delta|channel-width|ocs-duration|
ocs-frequency|path-min|path-threshold|priority-meshpoint|sample-count|snr-del
ta|
signal-threshold|tolerance-period] [2.4GHZ|5GHz]
```

no acs	Reverts the automatic channel selection settings to default
channel-hold-time	Reverts channel hold time to default (1800 seconds)
channel-switch-delta	Reverts channel switch delta to default (10 dBm)
channel-width	Reverts channel width to default (auto)
ocs-duration	Reverts off -channel scan duration to default (50 milliseconds)
ocs-frequency	Reverts off -channel scan frequency to default (6 seconds)
path-min	Reverts the minimum root path metric to default (1000)
path-threshold	Reverts the root path metric threshold to default (1500)
priority-meshpoint	Disables the priority meshpoint configuration
sample-count	Reverts the sample count to default (5 samples)
snr-delta	Reverts the channel SNR delta to default (5 db)
signal-threshold	Reverts the signal strength threshold to default (-65 dB)
tolerance-period	Reverts the tolerance period to default (60 seconds)

```
no exclude wired-peer mint-level-1
```

no exclude wired-peer	Disables exclusion of wired peers (wired mesh devices) with MiNT level-1 link

```
no hysteresis [min-threshold|period|root-sel-snr-delta|snr-delta]
```

no hysteresis [min-threshold|period|root-sel-snr-delta|snr-delta]	Removes the configured path selection SNR hysteresis values

```
no monitor [critical-resource|primary-port-link-loss]
```

no monitor critical-resource	Disables critical resource down event monitoring
no monitor primary-port-link-loss	Disables primary port link loss event monitoring

```
no [path-method|root {select-method}]
```

no root select-method	Removes the configuration of this meshpoint device as a root meshpoint. Also allows you to disable dynamic mesh selection (if enabled).
no path-method	Resets the path selection method (path to the root node) to default (uniform)

```
no root-select cost-root]
```

no root-select cost-root	Removes the selected meshpoint-device as the cost-root

```
no preferred [interface|root|neighbor]
```

no preferred	Resets the preferred path configuration
interface	Resets the preferred interface
root	Resets the preferred root to *none*
neighbor	Resets the preferred neighbor to *none*

Example

```
rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#show context
 meshpoint-device test
  name test
  root
  preferred root 22-33-44-55-66-77
  preferred neighbor 11-22-33-44-55-66
  preferred interface 5GHz
  monitor critical-resource action no-root
rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#

rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#no monitor
critical-resource
rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#no preferred
neighbor
rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#no root
rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#no preferred
interface

rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#show context
 meshpoint-device test
  name test
  no root
  preferred root 22-33-44-55-66-77
rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#
```

Chapter

PASSPOINT POLICY 28

There has been an exponential increase in the number and types of Wi-Fi mobile devices being used globally, resulting in a phenomenal growth in the data traffic volume. Consequently, the demand for secure, quick, and unlicensed access to public Wi-Fi hotspots, capable of handling this sudden influx of mobile data traffic, has been increasing. However, public hotspots have certain intrinsic usability issues, such as network discovery and selection, traffic prioritization, roaming capabilities, user authentication etc. The IEEE 802.11u standards (includes Hotspot 2.0 protocol extensions) were introduced to address these issues.

Hotspot 2.0 is a Wi-Fi Alliance standard that enables interoperability between clients, infrastructure, and operators. It makes a portion of the IEEE 802.11u standard mandatory and adds Hotspot 2.0 extensions that allow clients to query a network before actually attempting to join it. For example, you are using a laptop at an airport and have a list of SSIDs to select from. You will have to first identify the SSID you have the credentials for and then connect to the network. This can be time consuming. In such a scenario, a Hotspot 2.0 enabled device would present only those SSIDs for which you possess credentials. In short Hotspot 2.0 allows devices to query a network for configuration details, such as WAN metrics, network type, hotspot service provider details, and domain names without actually connecting to the network.

Hotspot 2.0 enabled clients can identify a Hotspot 2.0 capable *access point* (AP) from the new elements present in the APs beacon/probe messages. Having ascertained that an AP is Hotspot 2.0 capable, the client uses action frames to send an *Access Network Query Protocol* (ANQP) query inside a *Generic Advertisement Service* (GAS) request. The AP responds with an action frame containing an ANQP response within a GAS response. Based on this response the mobile device determines the type of credentials needed to log on to the AP.

The Brocade Mobility 5.5 Wi-Fi Alliance implementation defines a passpoint policy that allows a single or a set of Hotspot 2.0 configuration to be global and referenced by the devices that use it. This policy is applied to APs to make them Hotspot 2.0 Wi-Fi Alliance compliant. The passpoint policy is mapped to a WLAN. However, only primary WLANs on a BSSID will have their passpoint policy configuration used. For more information, see “use” on page 355.

To migrate to the passpoint policy configuration mode, use the following command:

```
<DEVICE>(config)#passpoint-policy <POLICY-NAME>

rfs4000-229D58(config)#passpoint-policy test
rfs4000-229D58(config-passpoint-policy-test)#

rfs4000-229D58(config-passpoint-policy-test)#?
Passpoint Policy Mode commands:
  3gpp                  Configure a 3gpp plmn (public land mobile network) id
  access-network-type    Set the access network type for the hotspot
  connection-capability  Configure the connection capability for the hotspot
  domain-name            Add a domain-name for the hotspot
  hessid                 Set a homogeneous ESSID value for the hotspot
  internet               Advertise the hotspot having internet access
  ip-address-type        Configure the advertised ip-address-type
  nai-realm              Configure a NAI realm for the hotspot
  net-auth-type          Add a network authentication type to the hotspot
```

```
  no                    Negate a command or set its defaults
  operator              Add configuration related to the operator of the
                        hotspot
  roam-consortium       Add a roam consortium for the hotspot
  venue                 Set the venue parameters of the hotspot
  wan-metrics           Set the wan-metrics of the hotspot

  clrscr                Clears the display screen
  commit                Commit all changes made in this session
  do                    Run commands from Exec mode
  end                   End current mode and change to EXEC mode
  exit                  End current mode and down to previous mode
  help                  Description of the interactive help system
  revert                Revert changes
  service               Service Commands
  show                  Show running system information
  write                 Write running configuration to memory or terminal

rfs4000-229D58(config-passpoint-policy-test)#
```

passpoint-policy

PASSPOINT POLICY

The following table summarizes passpoint policy configuration mode commands.

TABLE 26 Hotspot-Policy-Config Commands

Command	Description	Reference
3gpp	Configures a *3rd Generation Partnership Project* (3gpp) *Public Land Mobile Network* (PLMN) ID	page 1307
access-network-type	Configures the access network type element in this hotspot	page 1308
connection-capability	Configures the connection capability element in this passpoint policy	page 1309
domain-name	Configures the RF Domains to which this hotspot is applicable	page 1310
hessid	Configures the *Homogeneous Extended Service Set Identifier* (HESSID) for a specified hotspot zone	page 1311
internet	Advertises the availability of Internet access in this hotspot	page 1312
ip-address-type	Advertises the IP address type used in this hotspot.	page 1312
nai-realm	Configures a *Network Access Identifier* (NAI) realm name and enters its configuration mode	page 1314
net-auth-type	Configures the network authentication type used in this hotspot	page 1317
no	Removes or reverts passpoint policy configuration	page 1318
operator	Configures the operator friendly name for this hotspot	page 1320
roam-consortium	Configures the list of Roaming Consortium *Organization Identifiers* (OIs) supported on this hotspot	page 1321
venue	Configures the venue group and type for this passpoint policy	page 1322
wan-metrics	Configures the WAN performance metrics for this hotspot	page 1326
clrscr	Clears the display screen	page 385
commit	Commits (saves) changes made in the current session	page 386

TABLE 26 Hotspot-Policy-Config Commands

Command	Description	Reference
end	Ends and exits the current mode and moves to the PRIV EXEC mode	page 234
exit	Ends the current mode and moves to the previous mode	page 387
help	Displays the interactive help system	page 387
revert	Reverts changes to their last saved configuration	page 394
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 394
show	Displays running system information	page 429
write	Writes information to memory or terminal	page 425

3gpp

passpoint-policy

Configures a *3rd Generation Partnership Project* (3GPP) *Public Land Mobile Network* (PLMN) information. The 3GPP PLMN information is a combination of the *Mobile Country Code* (MCC) and *Mobile Network Code* (MNC). This MCC and MNC combination uniquely identifies a cellular operator. For example, Telstar Corporation Ltd. in Australia is identified by MCC 505 and MNC 001.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
3gpp mcc <MOBILE-COUNTRY-CODE> mnc <MOBILE-NETWORK-CODE> {description <LINE>}
```

Parameters

```
3gpp <1-20> mcc <MOBILE-COUNTRY-CODE> mnc <MOBILE-NETWORK-CODE> {description
<LINE>}
```

3gpp	Configures the 3GPP PLMN information that is returned in response to an ANQP query
mcc <MOBILE-COUNTRY-CODE>	Specifies the MCC. The MCC is a two or three digit decimal value. For example, the MCC for Australia is 505.
mnc <MOBILE-NETWORK-CODE>	Specifies the MNC. The MNC is a two or three decimal value used in combination with the MCC to uniquely identify a mobile network operator. The MNC and MCC combination (also known as the MCC/MNC tuple) forms the first five or six digits of the *International Mobile Subscriber's Identity* (IMSI). If the MCC and MNC values are not configured, the hotspot will not return the element in an ANQP capability request and ignores any ANQP query for the element.
description <LINE>	Optional. Configures a description that uniquely identifies this PLMN. Provide a description not exceeding 64 characters in length.

Example

```
rfs4000-229D58(config-passpoint-policy-test)#3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```

```
rfs4000-229D58(config-passpoint-policy-test)#3gpp mcc 310 mnc 970
rfs4000-229D58(config-passpoint-policy-test)#

rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
 3gpp mcc 310 mnc 970
 3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```

Related Commands:

no	Removes the specified 3gpp PLMN information and its corresponding MCC/MNC settings

access-network-type

passpoint-policy

Configures the access network type for this hotspot. The beacons and probe responses communicate the type of hotspot (public, private, guest-use, emergency etc.) to clients seeking access.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
access-network-type
[chargeable-public|emergency-services|experimental|free-public|
          personal-device|private|private-guest|wildcard]
```

Parameters

```
access-network-type
[chargeable-public|emergency-services|experimental|free-public|
personal-device|private|private-guest|wildcard]
```

access-network-type	Select the access network type for this hotspot. The options are: • chargeable-public – The network type is a chargeable public network • emergency-services – The network is used to provide emergency services only • experimental – The network is used for test or experimental purposes only • free-public – The network type is a free public • personal-device – The network is used for personal devices only • private – The network is a private network • private-guest – The network is a private network with guest access (default setting) • wildcard – Includes all access network types If the network type is set to chargeable-public, probe responses advertise this hotspot as a chargeable-public hotspot.

Example

```
rfs4000-229D58(config-passpoint-policy-test)#access-network-type
chargeable-public
```

```
rfs4000-229D58(config-passpoint-policy-test)#

rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
 access-network-type chargeable-public
 3gpp mcc 310 mnc 970
 3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```

Related Commands:

no	Reverts to the default access network type setting (private)

connection-capability

passpoint-policy

Configures the connection capability element in this passpoint policy. When configured, it communicates which ports are open or closed on the Hotspot, in response to an ANQP query.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
connection-capability [ftp|http|icmp|ip-protocol|ipsec-vpn|pptp-vpn|sip|ssh|
tls-vpn]

connection-capability [ftp|http|icmp|ipsec-vpn|pptp-vpn|sip|ssh|tls-vpn]
          [closed|open|unknown]

connection-capability ip-protocol <0-255> port <0-65535> [closed|open|unknown]
```

Parameters

```
connection-capability [ftp|http|icmp|ipsec-vpn|pptp-vpn|sip|ssh|tls-vpn]
[closed|open|unknown]
```

connection-capability	Configures the connection capability element in this passpoint policy
ftp	Specifies the protocol type as FTP. Configures TCP port 20.
http	Specifies the protocol type as HTTP. Configures TCP port 80.
icmp	Specifies the protocol type as ICMP
ipsec-vpn	Specifies the protocol type as IPSEC VPN. Configures ESP and UDP ports 500 and 4500.
pptp-vpn	Specifies the protocol type as PPTP VPN. Configures TCP port 1723.
sip	Specifies the protocol type as SIP. Configures TCP port 5060 and UDP port 5060.
ssh	Specifies the protocol type as SSH. Configures TCP port 20

tls-vpn	Specifies the protocol type as TLS VPN. Configures TCP port 443.
port <0-65535> [closed|open|unknown]	After specifying the protocol type, specify the port (associated with the selected protocol) and its status. • closed – Specifies that the port(s) is/are closed • open – Specifies that the port(s) is/are open • unknown – Specifies that the port(s) status is not known When the connection capability element is not configured, the hotspot does not return the element in an ANQP capability request and ignores any ANQP query for the element.

`connection-capability ip-protocol <0-255> port <0-65535> [closed|open|unknown]`

connection-capability	Configures the connection capability element in this passpoint policy
ip-protocol <0-255>	Identifies the IP protocol by the protocol's number. For example, for *simple message protocol* (SMP) specify 121.
port <0-65535> [closed|open|unknown]	After specifying the IP protocol type, specify the port number. • port <0-65535> – Select a port for the IP protocol identified. After specifying the port number, specify the port status. • closed – Specifies that the port(s) is/are closed • open – Specifies that the port(s) is/are open • unknown – Specifies that the port(s) status is not known When the connection capability element is not configured, the hotspot does not return the element in an ANQP capability request and ignores any ANQP query for the element.

Example

```
rfs4000-229D58(config-passpoint-policy-test)#connection-capability 1
ip-protocol 2 port 10 closed
rfs4000-229D58(config-passpoint-policy-test)#

rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
 access-network-type chargeable-public
 connection-capability ip-protocol 2 port 10 closed
 3gpp mcc 310 mnc 970
 3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```

Related Commands:

no	Removes the configured connection capability element on the passpoint policy

domain-name

passpoint-policy

Configures the RF Domain(s) that are returned in response to an ANQP query

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
domain-name <DOMAIN-NAME>
```

Parameters

```
domain-name <DOMAIN-NAME>
```

domain-name <DOMAIN-NAME>	Specify the RF Domain name An hotspot can be applied across multiple RF Domains.

Example

```
rfs4000-229D58(config-passpoint-policy-test)#domain-name TechPubs
rfs4000-229D58(config-passpoint-policy-test)#

rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
 access-network-type chargeable-public
 connection-capability ip-protocol 2 port 10 closed
 domain-name TechPubs
 3gpp mcc 310 mnc 970
 3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```

Related Commands:

no	Removes the RF Domain mapped to this passpoint policy

hessid

passpoint-policy

Configures the *Homogeneous Extended Service Set Identifier* (HESSID) for the hotspot. The HESSID uniquely identifies a hotspot provider within a zone. This is essential in zones (such as an airport or shopping mall) having multiple hotspot service providers with overlapping coverage.

An HESSID is a 6 (six) byte identifier that uniquely identifies a set of APs belonging to the same network and exhibiting same network behaviour. It is the BSSID (MAC address) of one of the devices (AP) in the zone. When not configured, the radio's BSSID is used as the HESSID.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
hessid <MAC>
```

Parameters

```
hessid <MAC>
```

hessid <MAC>	Specify a unique 6 (six) byte identifier for this passpoint policy.

Example

```
rfs4000-229D58(config-passpoint-policy-test)#hessid 00-23-68-88-0D-A7
rfs4000-229D58(config-passpoint-policy-test)#

rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
 access-network-type chargeable-public
 connection-capability ip-protocol 2 port 10 closed
 domain-name TechPubs
 hessid 00-23-68-88-0D-A7
 3gpp mcc 310 mnc 970
 3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```

Related Commands:

no	Removes the HESSID configured with this passpoint policy and reverts back to using the radio's BSSID

internet

passpoint-policy

Advertises the availability of Internet access on this hotspot. The Internet bit in the hotspot's beacon and probe responses indicates if Internet access is available or not. By default this feature is enabled.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
internet
```

Parameters

None

Example

```
rfs4000-229D58(config-passpoint-policy-test)#internet
rfs4000-229D58(config-passpoint-policy-test)#
```

Related Commands:

no	Removes Internet access on this passpoint policy

ip-address-type

passpoint-policy

Advertises the IP address type used in this hotspot. This information is returned in response to ANQP queries.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
ip-address-type [ipv4|ipv6]

ip-address-type ipv4 [double-nat|not-available|port-restricted|

port-restricted-double-nat|port-restricted-single-nat|public|single-nat|unkno
wn]

ip-address-type ipv6 [available|not-available|unknown]
```

Parameters

```
ip-address-type ipv4 [double-nat|not-available|port-restricted|
port-restricted-double-nat|port-restricted-single-nat|public|single-nat|unkno
wn]
```

ip-address-type ipv4	Configures the as IPv4 address type availability information
double-nat	Specifies double NATed private IPv4 address is available
not-available	Specifies IPv4 address is not available
port-restricted	Specifies port-restricted IPV4 address is available
port-restricted-double-nat	Specifies port-restricted IPv4 address and double NATed IPv4 address is available
port-restricted-single-nat	Specifies port-restricted IPv4 address and single NATed IPv4 address is available
public	Specifies public IPv4 address is available
single-nat	Specifies single NATed IPv4 address is available
unknown	Specifies no information configured regarding the IPv4 address availability

```
ip-address-type ipv6 [available|not-available|unknown]
```

ip-address-type ipv6	Configures the IPv6 address type availability information
available	Specifies IPv6 address is available
not-available	Specifies IPv6 address is not available
unknown	Specifies no information configured regarding the IPv6 address availability

Example

```
rfs4000-229D58(config-passpoint-policy-test)#ip-address-type ipv6 available
rfs4000-229D58(config-passpoint-policy-test)#

rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
 access-network-type chargeable-public
 connection-capability ip-protocol 2 port 10 closed
```

```
 domain-name TechPubs
 hessid 00-23-68-88-0D-A7
 ip-address-type ipv6 available
 3gpp mcc 310 mnc 970
 3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```

Related Commands:

no	Removes the IP address type configured for this passpoint policy

nai-realm

passpoint-policy

A *Network Access Identifier* (NAI) realm element in the passpoint policy identifies a hotspot service provider by the unique NAI realm name.

The following table lists NAI realm configuration mode commands.

Command	Description	Reference
nai-realm	Creates a NAI realm name for this hotspot and enters its configuration mode	page 1314
nai-realm-config-mode commands	Invokes the NAI realm configuration mode commands	page 1315

nai-realm

nai-realm

Configures a NAI realm name and enters its configuration mode. The NAI realm name identifies the accessible hotspot service providers. You can configure a list of NAI realm names of service providers operating within a specific hotpsot zone.This NAI realm name list is presented in ANQP response to a NAI realm and NAI home realm query

The configured NAI realm name list is presented in ANQP response to a NAI realm and NAI home realm query.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
nai-realm <HOTSPOT2-NAI-REALM-NAME>
```

Parameters

```
nai-realm <HOTSPOT2-NAI-REALM-NAME>
```

nai-realm <HOTSPOT2-NAI-REALM-NAME>	Configures the NAI realm name for this passpoint policy • <HOTSPOT2-NAI-REALM-NAME> – Specify the NAI realm name for this passpoint policy.

Example

```
rfs4000-229D58(config-passpoint-policy-test)#nai-realm mail.example.com
rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.example.com)#

rfs4000-229D58(config-passpoint-policy-test)#nai-realm mail.testrealm.com
rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.testrealm.com)#

rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.example.com)#?
Hotspot2 NAI Realm Mode commands:
  eap-method  Set an eap method
  no          Negate a command or set its defaults

  clrscr      Clears the display screen
  commit      Commit all changes made in this session
  do          Run commands from Exec mode
  end         End current mode and change to EXEC mode
  exit        End current mode and down to previous mode
  help        Description of the interactive help system
  revert      Revert changes
  service     Service Commands
  show        Show running system information
  write       Write running configuration to memory or terminal

rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.example.com)#exit

rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
 access-network-type chargeable-public
 connection-capability ip-protocol 2 port 10 closed
 domain-name TechPubs
 hessid 00-23-68-88-0D-A7
 ip-address-type ipv6 available
 nai-realm mail.example.com
 nai-realm mail.testrealm.com
 3gpp mcc 310 mnc 970
 3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```

Related Commands:

no	Removes the NAI realm name configured for this passpoint policy

nai-realm-config-mode commands

nai-realm

The following table summarizes NAI realm configuration mode commands.

Command	Description	Reference
eap-method	Specifies the *Extensible Authentication Protocol* (EAP) authentication mechanisms supported by each of the service providers associated with this passpoint policy	page 1315

eap-method

nai-realm-config-mode commands

Specifies the EAP authentication mechanisms supported by each of the service providers associated with this passpoint policy

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
eap-method <1-10>
[<1-255>|fast|gtc|identity|ikev2|ms-auth|mschapv2|otp|peap|psk|
          rsa-public-key|sim|tls|ttls] auth-param
[credential|expanded-eap|expanded-inner-eap|
          inner-eap|non-eap-inner|tunn-eap-credential|vendor]
```

Parameters

```
eap-method <1-10>
[<1-255>|fast|gtc|identity|ikev2|ms-auth|mschapv2|otp|peap|psk|
       rsa-public-key|sim|tls|ttls] auth-param [credential|expanded-eap|
expanded-inner-eap|
inner-eap|non-eap-inner|tunn-eap-credential|vendor]
```

eap-method <1-10>	Creates an EAP authentication method and assigns it an index number • <1-10> – Specify a identifier for this EAP method from 1 - 10. A maximum of 10 (ten) authentication methods can be specified for every NAI realm. After creating the EAP authentication method, specify the associated authentication mechanisms (method types).
<1-255>	Identifies the EAP authentication method type from the corresponding *Internet Assigned Numbers Authority* (IANA) number <1-255> – Specify the IANA identity number for the authentication protocol from 1 -255.
fast	Specifies the EAP authentication method type as *Flexible Authentication via Secure Tunneling* (FAST)
gtc	Specifies the EAP authentication method type as *Generic Token Card* (GTC)
identity	Specifies the EAP authentication method type as Identification
ikev2	Specifies the EAP authentication method type as *Internet Key Exchange Protocol version 2* (IKEv2)
ms-auth	Specifies the EAP authentication method type as *Microsoft Authentication* (MS-Auth)
mschapv2	Specifies the EAP authentication method type as *Microsoft Challenge Handshake Authentication Protocol* version 2(MSCHAPv2)
opt	Specifies the EAP authentication method type as *One Time Password* (OTP)
peap	Specifies the EAP authentication method type as *Protected Extensible Authentication Protocol* (PEAP)
psk	Specifies the EAP authentication method type as *Pre-shared Key* (PSK)
rsa-public-key	Specifies the EAP authentication method type as RSA public key protocol
sim	Specifies the EAP authentication method type as GSM *Subscriber Identity Module* (SIM)
tls	Specifies the EAP authentication method type as *Transport Layer Security* (TLS)
ttls	Specifies the EAP authentication method type as *Tunneled Transport Layer Security* (TTLS)
auth-param	After specifying the EAP authentication method type, specify the authentication parameters. These parameters depend on the EAP authentication mechanism selected.

Example

```
The following examples show four EAP authentication methods associated with
the NAI realm 'mail.example.com'. Each method supports a different EAP
authentication mechanism:

rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.example.com)#eap-m
ethod 1 ttls auth-param vendor hex 00001E
rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.example.com)#

rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.example.com)#eap-m
ethod 2 rsa-public-key auth-param credential cert
rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.example.com)#

rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.example.com)#eap-m
ethod 3 otp auth-param credential username-password
rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.example.com)#

rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.example.com)#eap-m
ethod 4 peap auth-param credential cert
rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.example.com)#

rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.example.com)#show
context
 nai-realm mail.example.com
  eap-method 1 ttls auth-param vendor hex 00121F
  eap-method 2 rsa-public-key auth-param credential cert
  eap-method 3 otp auth-param credential username-password
  eap-method 4 peap auth-param credential cert
rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.example.com)#
```

net-auth-type

passpoint-policy

Configures the network authentication type used in this hotspot. The details configured are returned in response to an ANQP query.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
net-auth-type [accept-terms|dns-redirect|http-redirect|online-enroll] {url
<URL>}
```

Parameters

```
net-authtype [accept-terms|dns-redirect|http-redirect|online-enroll] {url
<URL>}
```

net-auth-type	Specifies the network authentication type used with this passpoint policy. The options are: accept-terms, dns-redirect, http-redirect, and online-enroll
accept-terms	Enables user acceptance of terms and conditions

dns-redirect	Enables DNS redirection of user
http-redirect	Enables HTTP redirection of user
online-enroll	Enables online user enrolment
url <URL>	Optional. Specify the location for each of above network authentication types.

Example

```
rfs4000-229D58(config-passpoint-policy-test)#net-auth-type accept-terms url
"www.motorolasolutions.com"
rfs4000-229D58(config-passpoint-policy-test)#

rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
 access-network-type chargeable-public
 connection-capability ip-protocol 2 port 10 closed
 domain-name TechPubs
 hessid 00-23-68-88-0D-A7
 ip-address-type ipv6 available
 nai-realm mail.example.com
  eap-method 1 ttls auth-param vendor hex 00001E
  eap-method 2 rsa-public-key auth-param credential cert
  eap-method 3 otp auth-param credential username-password
  eap-method 4 peap auth-param credential cert
 nai-realm mail.testrealm.com
 net-auth-type accept-terms url www.motorolasolutions.com
 3gpp mcc 310 mnc 970
 3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```

Related Commands:

no	Removes the network authentication type configured with this passpoint policy

no

passpoint-policy

Removes or reverts the passpoint policy settings

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
no
[3gpp|access-network-type|connection-capability|domain-name|hessid|internet|

ip-address-type|nai-realm|net-auth-type|operator|roam-consortium|venue|wan-me
trics]
```

Parameters

```
no
[3gpp|access-network-type|connection-capability|domain-name|hessid|internet|
ip-address-type|nai-realm|net-auth-type|operator|roam-consortium|venue|wan-me
trics]
```

no 3gpp	Removes the specified 3GPP PLMN ID and its corresponding MCC/MNC settings
no access-network-type	Reverts to the default access network type setting (private)
no connection-capability	Removes the configured connection capability element on the hotspot
no domain-name	Removes the RF Domain mapped to the hotspot
no hessid	Removes the HESSID configured on the hotspot and reverts back to using the radio's BSSID
no internet	Removes Internet access on this hotspot
no ip-address-type	Removes the IP address type applicable on this hotspot
no nai-realm	Removes the NAI realm name configured for this hotspot
no net-auth-type	Removes the network authentication type configured with this hotspot
no operator	Removes the operator friendly name configured for this hotspot
no roam-consortium	Removes the Roaming Consortium OIs supported on this hotspot
no venue	Removes the venue group and type configured with this hotspot
no wan-metrics	Removes the WAN metrics configuration on this hotspot

Example

The following example shows the passpoint policy 'test' settings before the 'no' commands are executed:

```
rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
 access-network-type chargeable-public
 connection-capability ip-protocol 2 port 10 closed
 domain-name TechPubs
 hessid 00-23-68-88-0D-A7
 ip-address-type ipv6 available
 nai-realm mail.example.com
  eap-method 1 ttls auth-param vendor hex 00001E
  eap-method 2 rsa-public-key auth-param credential cert
  eap-method 3 otp auth-param credential username-password
  eap-method 4 peap auth-param credential cert
 nai-realm mail.testrealm.com
 net-auth-type accept-terms url www.motorolasolutions.com
 3gpp mcc 310 mnc 970
 3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#

rfs4000-229D58(config-passpoint-policy-test)#no access-network-type
rfs4000-229D58(config-passpoint-policy-test)#no hessid
rfs4000-229D58(config-passpoint-policy-test)#no nai-realm mail.example.com
rfs4000-229D58(config-passpoint-policy-test)#no 3gpp mcc 310 mnc 970
rfs4000-229D58(config-passpoint-policy-test)#no internet

rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
 connection-capability ip-protocol 2 port 10 closed
 domain-name TechPubs
 no internet
 ip-address-type ipv6 available
```

```
 nai-realm mai.testrealm.com
 net-auth-type accept-terms url www.motorolasolutions.com
 3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```

operator

passpoint-policy

Configures the operator friendly name for this hotspot. The name can be configured in English or in any language other than English. When the name is specified in English, the system allows an ASCII input. If you are using a language other than English, first specify the ISO-639 language code, and then specify the name as an hexadecimal code.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
operator name [<OPERATOR-NAME>|iso-lang <ISO-LANG-CODE>]

operator name <OPERATOR-NAME>
operator name iso-lang <ISO-LANG-CODE> <OPERATOR-NAME>
```

Parameters

```
operator name <OPERATOR-NAME>
```

name <OPERATOR-NAME>	Configures the operator's name in English • <OPERATOR-NAME> – Specify the operator friendly name in ASCII format.

```
operator name iso-lang <ISO-LANG-CODE> <OPERATOR-NAME>
```

name iso-lang <ISO-LANG-CODE> <OPERATOR-NAME>	Configures a non-English operator's name • iso-lang <ISO-LANG-CODE> – Identifies the language by its ISO 639 language code (for example, 'chi-chinese' or 'spa-spanish'). • <ISO-LANG-CODE> – Specify the 3 character iso-639 language code (for example, 'chi-chinese' or 'spa-spanish • <OPERATOR-NAME> – Specifies the operator's name as a hexadecimal code

Example

```
rfs4000-229D58(config-passpoint-policy-test)#operator name emergencyservices
rfs4000-229D58(config-passpoint-policy-test)#

rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
 connection-capability ip-protocol 2 port 10 closed
 domain-name TechPubs
 no internet
 ip-address-type ipv6 available
 nai-realm mai.testrealm.com
 net-auth-type accept-terms url www.motorolasolutions.com
 operator name emergencyservices
```

```
 3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```

Related Commands:

no	Removes the operator friendly name configured for this passpoint policy

roam-consortium

passpoint-policy

Configures a list of *Roaming Consortium* (RC) *Organization Identifiers* (OIs) supported on this hotspot. The beacons and probe responses communicate this Roaming Consortium list to devices. This information enables a device to identify the networks available through this AP.

Each OI identifies a either a group of *Subscription Service Providers* (SSPs) or a single SSP.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
roam-consortium hex <WORD>
```

Parameters

```
roam-consortium hex <WORD>
```

roam-consortium hex <WORD>	Adds a Roaming Consortium OI to this hotspot in hexadecimal format • <WORD> – Specify the Roaming Consortium OI in hexadecimal format (should not exceed 128 characters)
hex <WORD>	Configures a hexadecimal input • <WORD> – Specify the Roaming Consortium OI in hexadecimal format (should not exceed 128 characters)

Example

```
rfs4000-229D58(config-passpoint-policy-test)#roam-consortium hex 223344
rfs4000-229D58(config-passpoint-policy-test)#

rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
 connection-capability ip-protocol 2 port 10 closed
 domain-name TechPubs
 no internet
 ip-address-type ipv6 available
 nai-realm mai.testrealm.com
 net-auth-type accept-terms url www.motorolasolutions.com
 operator name emergencyservices
 roam-consortium hex 223344
 3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```

Related Commands:

no	Removes the Roaming Consortium OIs supported on this passpoint policy

venue

passpoint-policy

Configures the venue where this hotspot is located. The hotspot venue configuration informs prospective clients about the hotspot's nature of activity, such as educational, institutional, residential etc.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
venue [group|name]

venue group
[assembly|business|educational|industrial|institutional|mercantile|
          outdoor|residential|storage|unspecified|utility-and-misc|vehicular]
type

venue name [<VENUE-NAME>|iso-lang]
venue name <VENUE-NAME>
venue name iso-lang <ISO-LANG-CODE> <VENUE-NAME>
```

Parameters

```
venue group
[assembly|business|educational|industrial|institutional|mercantile|
outdoor|residential|storageunspecified|utility-and-misc|vehicular] type
```

venue group	Configures the venue group associated with this hotspot
assembly type	Configures the venue group as assembly (1). This hotspot type is applicable to public assembly venues. • type – Specifies the venue type for this group. The options are: • <0-255> – Specifies an unlisted venue type number from 0 -255 • amphitheater – Specifies the venue type as amphitheater (4) • amusement-park – Specifies the venue type as amusement park (5) • arena – Specifies the venue type as arena (1) • bar – Specifies the venue type as bar (12) • coffee-shop – Specifies the venue type as a coffee shop (13) • convention-centre – Specifies the venue type as a convention center (7) • emergency-coordination-center – Specifies the venue type as a emergency coordination center (15) • library – Specifies the venue type as a library (8) • museum – Specifies the venue type as a museum (9) • passenger-terminal – Specifies the venue type as a passenger terminal (3) • place-of-worship – Specifies the venue type as a place of worship (6) • restaurant – Specifies the venue type as a restaurant (10) • stadium – Specifies the venue type as a stadium (2) • theater – Specifies the venue type as a theater (11) • unspecified – Specifies the venue type as not specified (0) • zoo – Specifies the venue type as a zoo (14)
business type	Configures the venue group as business (2). This hotspot type is applicable to business venues. • type – Specifies the venue type for this group. The options are: • <0-255> – Specifies an unlisted venue type number from 0 -255 • attorney – Specifies the venue type as the attorney's office (9) • bank – Specifies the venue type as a bank (2) • doctor – Specifies the venue type as a doctor or dentist's office (1) • fire-station – Specifies the venue type as a fire station (3) • police-station – Specifies the venue type as a police station (4) • post-office – Specifies the venue type as a post office (5) • professional-office – Specifies the venue type as a professional office (7) • research-and-development-facility – Specifies the venue type as a research facility (8) • unspecified – Specifies the venue type as not specified (0)
educational	Configures the venue group as educational (3). This hotspot type is applicable to educational institutions. • type – Specifies the venue type for this group. The options are: • <0-255> – Specifies an unlisted venue type number from 0 -255 • school-primary – Specifies the venue type as a primary school (1) • school-secondary – Specifies the venue type as a secondary school (2) • university – Specifies the venue type as a university or college (3) • unspecified – Specifies the venue type as not specified (0)
industrial	Configures the venue group as industrial (4). This hotspot type is applicable to industrial venues. • type – Specifies the venue type for this group. The options are: • <0-255> – Specifies an unlisted venue type number from 0 -255 • factory – Specifies the venue type as a factory (1) • unspecified – Specifies the venue type as not specified (0)

institutional	Configures the venue group as institutional (4). This hotspot type is applicable to public health and other institutions.
	• type – Specifies the venue type for this group. The options are:
	  • <0-255> – Specifies an unlisted venue type number from 0 -255
	  • group-home – Specifies the venue type as a group-home (4)
	  • hospital – Specifies the venue type as a hospital (1)
	  • long-term-care – Specifies the venue type as a long term care facility (2)
	  • prison – Specifies the venue type as a prison or jail (5)
	  • rehab – Specifies the venue type as a rehabilitation facility (3)
	  • unspecified – Specifies the venue type as not specified (0)

mercantile	Configures the venue group as mercantile (6). This hotspot type is applicable to public mercantile venues.
	• type – Specifies the venue type for this group. The options are:
	  • <0-255> – Specifies an unlisted venue type number from 0 -255
	  • automotive – Specifies the venue type as a automotive service center (3)
	  • gas-station – Specifies the venue type as a gas station (5)
	  • grocery – Specifies the venue type as a grocery store (2)
	  • mall – Specifies the venue type as a shopping mall (4)
	  • retail – Specifies the venue type as a retail store (1)
	  • unspecified – Specifies the venue type as not specified (0)

outdoor	Configures the venue group as outdoor (11). This hotspot type is applicable to public outdoor venues.
	• type – Specifies the venue type for this group. The options are:
	  • <0-255> – Specifies an unlisted venue type number from 0 -255
	  • bus-stop – Specifies the venue type as a bus stop (5)
	  • city-park – Specifies the venue type as a city park (2)
	  • kiosk – Specifies the venue type as a kiosk (6)
	  • muni-mesh – Specifies the venue type as a muni-mesh (municipal wireless Wi-Fi) (1)
	  • rest-area – Specifies the venue type as a rest area (3)
	  • traffic-control – Specifies the venue type as a traffic control area (4)
	  • unspecified – Specifies the venue type as not specified (0)

residential	Configures the venue group as residential (7). This hotspot type is applicable to residential complexes.
	• type – Specifies the venue type for this group. The options are:
	  • <0-255> – Specifies an unlisted venue type number from 0 -255
	  • boarding-house – Specifies the venue type as a boarding-house (4)
	  • dorm – Specifies the venue type as a dormitory (3)
	  • hotel – Specifies the venue type as a hotel or motel (2)
	  • private – Specifies the venue type as a private residence (1)
	  • unspecified – Specifies the venue type as not specified (0)

storage	Configures the venue group as storage (8). This hotspot type is applicable to storage groups.
	• type – Specifies the venue type for this group. The options are:
	  • <0-255> – Specifies an unlisted venue type number from 0 -255
	  • unspecified – Specifies the venue type as not specified (0)

unspecified	Configures the venue group as unspecified (0)
	• type – Specifies the venue type for this group. The options are:
	  • <0-255> – Specifies an unlisted venue type number from 0 -255
	  • unspecified – Specifies the venue type as not specified (0)

utility-and-misc	Configures the venue group as utility and miscellaneous (8) • type – Specifies the venue type for this group. The options are: • <0-255> – Specifies an unlisted venue type number from 0 -255 • unspecified – Specifies the venue type as not specified (0)
vehicular	Configures the venue group as vehicular (7). This hotspot type is applicable to mobile venues. • type – Specifies the venue type for this group. The options are: • <0-255> – Specifies an unlisted venue type number from 0 -255 • airplane – Specifies the venue type as an airplane (2) • auto – Specifies the venue type as an automobile or truck (1) • bus – Specifies the venue type as a bus (3) • ferry – Specifies the venue type as a ferry (5) • motor-bike – Specifies the venue type as a motor bike (7) • ship – Specifies the venue type as a ship or boat (5) • train – Specifies the venue type as a train (6) • unspecified – Specifies the venue type as not specified (0)

```
operator name <VENUE-NAME>
```

name <WORD>	Configures the venue name in English • <WORD> – Specify the venue name in ASCII format.

```
operator name iso-lang <ISO-LANG-CODE> <VENUE-NAME>
```

name iso-lang <ISO-LANG-CODE> <VENUE-NAME>	Configures a non-English venue name • iso-lang <ISO-LANG-CODE> – Identifies the language by its ISO 639 language code (for example, 'chi-chinese' or 'spa-spanish'). • <ISO-LANG-CODE> – Specify the 3 character iso-639 language code (for example, 'chi-chinese' or 'spa-spanish • <VENUE-NAME> – Specifies the venue name as a hexadecimal code

Example

```
rfs4000-229D58(config-passpoint-policy-test)#venue name PublicSchool
rfs4000-229D58(config-passpoint-policy-test)#

rfs4000-229D58(config-passpoint-policy-test)#venue group assembly type
coffee-shop
rfs4000-229D58(config-passpoint-policy-test)#

rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
 connection-capability ip-protocol 2 port 10 closed
 domain-name TechPubs
 no internet
 ip-address-type ipv6 available
 nai-realm mai.testrealm.com
 net-auth-type accept-terms url www.motorolasolutions.com
 operator name emergencyservices
 roam-consortium hex 223344
 venue group assembly type coffee-shop
 venue name PublicSchool
 3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```

Related Commands:

no	Removes the venue group and type configured with this passpoint policy

wan-metrics

passpoint-policy

Configures the WAN performance metrics for this hotspot. This command configures the upstream and downstream speeds associated with this hotspot. The upstream and downstream speed values (in Kbps) are estimates of the bandwidth available on the WAN. This information is returned in response to client ANQP query, and is useful for clients having a minimum and/or large bandwidth requirement.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 1220 Access Point, Brocade Mobility 71XX Access Point, Brocade Mobility 1240 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
wan-metrics down-speed <0-4294967295> up-speed <0-4294967295>
```

Parameters

```
wan-metrics down-speed <0-4294967295> up-speed <0-4294967295>
```

wan-metrics	Specifies the WAN metrics for the up and down traffic
down-speed <0-4294967295>	Configures the down stream traffic speed • <0-4294967295> – Specify a value from 0 - 4294967295 Kbps
up-speed <0-4294967295>	Configures the up stream traffic speed • <0-4294967295> – Specify a value from 0 - 4294967295 Kbps

Example

```
rfs4000-229D58(config-passpoint-policy-test)#wan-metrics down-speed 2000
up-speed 2000
rfs4000-229D58(config-passpoint-policy-test)#

rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
 connection-capability ip-protocol 2 port 10 closed
 domain-name TechPubs
 no internet
 ip-address-type ipv6 available
 nai-realm mai.testrealm.com
 net-auth-type accept-terms url www.motorolasolutions.com
 operator name emergencyservices
 roam-consortium hex 223344
 venue group assembly type coffee-shop
 venue name PublicSchool
 wan-metrics down-speed 2000 up-speed 2000
 3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```

Related Commands:

no	Removes the WAN metrics configuration on this passpoint policy

Chapter

FIREWALL LOGGING 29

This chapter summarizes firewall logging commands in the CLI command structure.

The firewall uses logging to send system messages to one or more logging destinations, where they can be collected, archived and reviewed.

Set the logging level to define which messages are sent to each of the target destinations.

Logging messages can be sent to any of the following destinations:

- The firewall console
- Telnet or SSH session to the firewall
- A temporary buffer internal to the firewall
- Syslog server
- E-mail addresses
- An FTP server

Firewall Log Terminology and Syslog Severity Levels

Abbreviation	Description
FTP	File transfer protocol
ACL	Access control list
Src MAC	Source MAC address
Dest MAC	Destination MAC address
LOGRULEHIT	ACL rule applied
PKT DROP	Packet drop
Src IP	Source IP address
Dest IP / Dst IP	Destination IP address
FWSTARTUP	Firewall enabled
DP	Destination port
SP	Source port
Matched Temporary Rule	This is a internal rule created to allow data traffic

Syslog Severity Level as Message	*Severity Level as Numeric*	*Description*
emergency	0	System is unusable
alert	1	Immediate action needed
critical	2	Critical condition

error	3	Error condition
warning	4	Warning condition
notification	5	Normal but significant condition
informational	6	Informational message
debugging	7	Debugging message

Date format in Syslog messages

The following output displays the wireless controller date in proper format:

```
rfs7000-37FABE(config)#Feb 07 11:09:00 2013: USER: cfgd: deleting session 4
rfs7000-37FABE
rfs7000-37FABE(config)#
rfs7000-37FABE(config)#Feb 07 11:09:17 2013: USER: cfgd: deleting session 5
```

The date format is Month <MMM> Date <DD> Time <HH:MM:SS> Year <YYYY>

```
Month is Feb
Date is 07
Time is 11:09:00
Year is 2013
```

To generate a date log, enable logging

For example, the following command has to be executed:

```
rfs7000-37FABE#clock set 11:09:17 07 Feb 2013
rfs7000-37FABE#
```

FTP data connection log

An ACL rule has to be applied and logging has to be enabled to generate a FTP data collection log.

The FTP connection is Control Connection

```
Feb 07 11:10:17 2013: %DATAPLANE-5-LOGRULEHIT: Matched ACL:ftpuser:ip Rule:0
Disposition:Allow Packet  Src MAC:<00-19-B9-6B-DA-77> Dst
MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.1.99 Dst
IP:192.168.2.102 Proto:6 Src Port:3014 Dst Port:21
Date is Feb 07
Time is 11:10:17
Year is 2013
Module name is DATAPLANE
Syslog Severity level is 5
Log ID is LOGRULEHIT
Log Message is Matched ACL
The Matching ACL  is FTPuser
IP Rule  sequence number is  0
Disposition is Allow Packet
Source MAC Address is 00-19-B9-6B-DA-77
Destination MAC Address is <00-15-70-81-91-6A>
Ethertype is  0x0800
Source IP Address is 192.168.1.99
Destination IP Address is  192.168.2.102
Protocol Type is 6
Source Port is 3014D
Destination Port is 21
```

NOTE
The same terminology is used across all logs.

The Data Connection in Active Mode

Feb 07 11:10:19 2013: %DATAPLANE-5-LOGRULEHIT: Matched Temporary Rule of FTP ALG. Disposition:Allow Packet Src MAC:<00-11-25-14-D9-E2> Dst MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.2.102 Dst IP:192.168.1.99 Proto:6 Src Port:20 Dst Port:3017.

The Data Connection in Passive Mode

Feb 07 11:14:31 2013: %DATAPLANE-5-LOGRULEHIT: Matched Temporary Rule of FTP ALG. Disposition:Allow Packet Src MAC:<00-19-B9-6B-DA-77> Dst MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.1.99 Dst IP:192.168.2.102 Proto:6 Src Port:3033 Dst Port:3894.

For example,

```
rfs7000-37FABE(config-mac-acl-test)#permit any any log rule-precedence 25
rfs7000-37FABE(config-mac-acl-test)#
```

UDP packets log

In both DHCP release and DHCP renew scenarios, the destination port 67 is logged.

DHCP Release

Feb 07 11:57:43 2013: %DATAPLANE-5-LOGRULEHIT: Matched ACL:ftpuser:ip Rule:1 Disposition:Allow Packet Src MAC:<00-11-25-14-D9-E2> Dst MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.2.102 Dst IP:172.16.31.196 Proto:17 Src Port:68 Dst Port:67.

DHCP Renew

Feb 07 11:58:48 2013: %DATAPLANE-5-LOGRULEHIT: Matched ACL:ftpuser:ip Rule:1 Disposition:Allow Packet Src MAC:<00-11-25-14-D9-E2> Dst MAC:<FF-FF-FF-FF-FF-FF> Ethertype:0x0800 Src IP:0.0.0.0 Dst IP:255.255.255.255 Proto:17 Src Port:68 Dst Port:67.

To generate a UDP packet log, an ACL rule has to be applied to UDP packets, and logging has to be enabled.

For example,

```
rfs7000-37FABE(config-ip-acl-test)#permit udp any any log rule-precedence 20
rfs7000-37FABE(config-ip-acl-test)#
```

ICMP type logs

The example below displays an ICMP Type as 13 and an ICMP Code as 0:

Feb 07 12:00:00 2013: %DATAPLANE-5-LOGRULEHIT: Matched ACL:ftpuser:ip Rule:0 Disposition:Allow Packet Src MAC:<00-11-25-14-D9-E2> Dst MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.2.102 Dst IP:192.168.1.103 Proto:1 ICMP Type:13 ICMP Code:0.

The below example displays an ICMP Type as 15 and an ICMP Code as 0:

Feb 07 12:00:07 2013: %DATAPLANE-5-LOGRULEHIT: Matched ACL:ftpuser:ip Rule:0 Disposition:Allow Packet Src MAC:<00-60-80-B0-C3-B3> Dst MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.1.104 Dst IP:192.168.2.102 Proto:1 ICMP Type:15 ICMP Code:0.

The below example displays an ICMP Type as 17 and an ICMP Code as 0:

Feb 07 12:00:25 2013: %DATAPLANE-5-LOGRULEHIT: Matched ACL:ftpuser:ip Rule:0 Disposition:Allow Packet Src MAC:<00-11-25-14-D9-E2> Dst MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.2.102 Dst IP:192.168.1.103 Proto:1 ICMP Type:17 ICMP Code:0.

The below example displays an ICMP Type as 18 and an ICMP Code as 0:

Feb 07 12 01:00:24 2013: %DATAPLANE-5-ICMPPKTDROP: Dropping ICMP Packet from 192.168.1.104 to 192.168.2.102, with ProtocolNumber:1 ICMP code 0 and ICMP type 18. Reason: no flow matching payload of ICMP Reply.

Module name is DATAPLANE

Syslog Severity level is 5

Log ID is ICMPPKTDROP

Log Message is Dropping ICMP Packet

To generate an ICMP log, an ACL rule has to be applied on ICMP packets, and logging has to be enabled.

For example, the following commands have to be executed:

```
rfs7000-37FABE(config-ip-acl-test)#permit icmp any any log rule-precedence 20
rfs7000-37FABE(config-ip-acl-test)#
```

ICMP type logs

The following example displays an ICMP Type as 3 and a Code as 3:

Feb 07 12:03:00 2013: %DATAPLANE-5-ICMPPKTDROP: Dropping ICMP Packet from 192.168.1.104 to 192.168.2.102, with ProtocolNumber:1 ICMP code 3 and ICMP type 3. Reason: no flow matching payload of ICMP Error.

Module name is DATAPLANE

Syslog Severity level is 5

Log ID is ICMPPKTDROP

Log Message is Dropping ICMP Packet

The following example displays an ICMP Type as 4 and a Code as 0:

Feb 07 12:04:06 2013: %DATAPLANE-5-ICMPPKTDROP: Dropping ICMP Packet from 192.168.1.104 to 192.168.2.102, with ProtocolNumber:1 ICMP code 0 and ICMP type 4. Reason: ICMP dest IP does not match inner source IP.

The following example displays an ICMP Type as 5 and a Code as 0:

Feb 07 12:05:00 2013: %DATAPLANE-5-ICMPPKTDROP: Dropping ICMP Packet from 192.168.1.104 to 192.168.2.102, with ProtocolNumber:1 ICMP code 0 and ICMP type 5. Reason: ICMP dest IP does not match inner source IP.

The following example displays an ICMP type as 11 and a Code as 0:

Feb 07 12:06:00 2013: %DATAPLANE-5-ICMPPKTDROP: Dropping ICMP Packet from 192.168.2.102 to 192.168.1.103, with ProtocolNumber:1 ICMP code 0 and ICMP type 11. Reason: ICMP dest IP does not match inner source IP.

The following example displays an ICMP type as 14 and a Code as 0:

Feb 07 12:07:00 2013: %DATAPLANE-5-ICMPPKTDROP: Dropping ICMP Packet from 192.168.1.104 to 192.168.2.102, with ProtocolNumber:1 ICMP code 0 and ICMP type 14. Reason: no flow matching payload of ICMP Reply.

The following example displays an ICMP type as 16 and a Code as 0:

Feb 07 12:10:11 2013: %DATAPLANE-5-ICMPPKTDROP: Dropping ICMP Packet from 192.168.1.104 to 192.168.2.102, with ProtocolNumber:1 ICMP code 0 and ICMP type 16. Reason: no flow matching payload of ICMP Reply.

To generate an ICMP log, logging has to be enabled.

For example, the following command has to be executed:

```
rfs7000-37FABE(config-fw-policy-default)#logging icmp-packet-drop all
rfs7000-37FABE(config-fw-policy-default)#
```

Raw IP Protocol logs

The following example displays a TCP header length as less than 20 bytes:

Feb 07 12:11:50 2013: %DATAPLANE-4-DOSATTACK: INVALID PACKET: TCP header length less than 20 bytes : Src IP : 192.168.2.102, Dst IP: 192.168.1.104, Src Mac: 00-11-25-14-D9-E2, Dst Mac: 00-15-70-81-91-6A, Proto = 6.

Module name is DATAPLANE

Syslog Severity level is 4

Log ID is DOSATTACK

Log Message is INVALID PACKET

Feb 07 12:12:00 2013: %DATAPLANE-5-MALFORMEDIP: Dropping IPv4 Packet from 192.168.2.102 to 192.168.1.104 Protocol Number: 6. Reason: malformed TCP header.

Module name is DATAPLANE

Syslog Severity level is 5

Log ID is MALFORMEDIP

Log Message is Dropping IPv4Packet

To generate a raw IP protocol log, logging has to be enabled.

For example, the following commands have to be executed:

```
rfs7000-37FABE(config-fw-policy-default)# logging verbose
rfs7000-37FABE(config-fw-policy-default)#
rfs7000-37FABE(config-fw-policy-default)# logging malformed-packet-drop all
rfs7000-37FABE(config-fw-policy-default)#
```

When logging verbose is enabled, the log is displayed as:

Feb 07 12:15:21 2013: %DATAPLANE-5-MALFORMEDIP: Dropping IPv4 Packet from 192.168.0.91 to 192.168.0.1 Protocol Number: 6 SrcPort: 22616 DstPort: 22616 Reason: no matching TCP flow.

Module name is DATAPLANE

Syslog Severity level is 5

Log ID is MALFORMEDIP

Log Message is Dropping IPv4Packet

Raw IP Protocol logs

The following example displays TCP without data:

Feb 07 12:16:50 2013: %DATAPLANE-4-DOSATTACK: INVALID PACKET: TCP header length less than 20 bytes : Src IP : 192.168.2.102, Dst IP: 192.168.1.104, Src Mac: 00-11-25-14-D9-E2, Dst Mac: 00-15-70-81-91-6A, Proto = 6.

Feb 07 12:16:55 2013: %DATAPLANE-5-MALFORMEDIP: Dropping IPv4 Packet from 192.168.2.102 to 192.168.1.104 Protocol Number: 6. Reason: malformed TCP header.

To generate a raw IP protocol log, logging has to be enabled.

For example, the following commands have to be executed:

```
rfs7000-37FABE(config-fw-policy-default)# logging verbose
rfs7000-37FABE(config-fw-policy-default)#
rfs7000-37FABE(config-fw-policy-default)# logging rawip-packet-drop all
rfs7000-37FABE(config-fw-policy-default)#
```

When logging verbose is enabled, the log is displayed as:

Feb 07 12:20:30 2013: %DATAPLANE-4-DOSATTACK: INVALID PACKET: TCP header length less than 20 byt es : Src IP : 192.168.0.91, Dst IP: 192.168.0.1, Src Mac: 00-16-36-05-72-2A, Dst Mac: 00-23-68-22-C8-6E, Proto = 6.

Feb 07 12:22:49 2013: %DATAPLANE-5-MALFORMEDIP: Dropping IPv4 Packet from 192.168.0.91 to 192.168.0.1 Protocol Number: 6 . Reason: malformed TCP header.

Module name is DATAPLANE

Syslog Severity level is 4

Log ID is DOSATTACK

Log Message is INVALID PACKET

Firewall startup log

The following example displays an enabled firewall. A firewall enabled message is displayed in **bold**.

System bootup time (via /proc/uptime) was 93.42 42.52

Please press Enter to activate this console. Feb 07 12:25:09 2013: %NSM-4-IFUP: Interface vlan2 is up

Feb 07 12:25:09 2013: KERN: vlan2: add 01:00:5e:00:00:01 mcast address to master interface.

Feb 07 12:25:09 2013: %NSM-4-IFUP: Interface vlan172 is up

Feb 07 12:25:09 2013: KERN: vlan172: add 01:00:5e:00:00:01 mcast address to master interface.

Feb 07 12:25:09 2013: %PM-6-PROCSTART: Starting process "/usr/sbin/lighttpd"

Feb 07 12:25:09 2013: %FILEMGMT-5-HTTPSTART: lighttpd started in external mode with pid 0

Feb 07 12:25:09 2013: %DAEMON-3-ERR: dhcrelay: interface allocate : vlan1

Feb 07 12:25:09 2013: %USER-5-NOTICE: FILEMGMT[1086]: FTP: ftp server stopped

Feb 07 12:25:09 2013: %DAEMON-3-ERR: dhcrelay: interface allocate : vlan1

Feb 07 12:25:09 2013: %DAEMON-3-ERR: dhcrelay: interface allocate : vlan1

Feb 07 12:25:09 2013: %DAEMON-3-ERR: dhcrelay: interface allocate : vlan2

Feb 07 12:25:09 2013: %DOT11-5-COUNTRY_CODE: Country of operation configured to in [India]

Feb 07 12:25:09 2013: %DIAG-6-NEW_LED_STATE: LED state message AP_LEDS_ON from module DOT11

Feb 07 12:25:09 2013: %PM-6-PROCSTART: Starting process "/usr/sbin/telnetd"

Feb 07 12:25:09 2013: %AUTH-6-INFO: sshd[1422]: Server listening on 0.0.0.0 port 22.

dataplane enabled

CCB:21:Firewall enabled

Feb 07 12:25:09 2013: %KERN-4-WARNING: dataplane enabled.

Feb 07 12:25:09 2013: %DATAPLANE-5-FWSTARTUP: Firewall enabled.

Feb 07 12:25:09 2013: USER: cfgd: handle_cluster_member_update

Feb 07 12:25:09 2013: USER: cfgd: ignoring, no cluster configured

Feb 07 12:25:09 2013: %PM-6-PROCSTART: Starting process "/usr/sbin/sshd"

Manual time change log

The following example displays the manual time change log. The clock is manually set to Feb 07 12:25:33 2013.

Log change in time

```
rfs7000-37FABE#show clock
2013-02-07 12:25:33 UTC
rfs7000-37FABE#
```

rfs7000-37FABE#clock set 12:25:33 07 Feb 2013

Feb 07 12:25:33 2013: %[S1]CFGD-6-SYSTEM_CLOCK_RESET: System clock reset, Time: 2013-02-07 12:45:00[S2]

```
rfs7000-37FABE#show clock
Feb 07 12:45:00 UTC 2013
rfs7000-37FABE#
```

To generate a time log, logging has to be enabled

For example, the following command has to be executed:

```
rfs7000-37FABE#clock set 12:45:00  07 Feb 2013
rfs7000-37FABE#
```

Firewall ruleset log

The following example displays the log changes as 'ACL_ATTACHED_ALTERED' when an ACL Rule is applied/removed on WLAN, VLAN, GE, and PORT-CHANNEL:

IP ACL IN on WLAN Attach

Feb 07 12:48:40 2013: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to wlan ICSA-testing is getting altered

USER: The user who is doing the change

session: means the session id of the user - one user can have multiple sessions running, so this explains from which session this change was done

ACL: Name of the ACL that has rules added/deleted

IP ACL IN on WLAN Remove

Feb 07 12:48:42 2013: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to wlan
ICSA-testing is getting altered.

IP ACL OUT on WLAN Attach

Feb 07 12:48:44 2013 2010: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to wlan
ICSA-testing is getting altered.

IP ACL OUT on WLAN Remove

Feb 07 12:48:50 2013 2010: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to wlan
ICSA-testing is getting altered.

MAC ACL IN on WLAN Attach

Feb 07 12:48:55 2013: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to wlan
ICSA-testing is getting altered.

MAC ACL IN on WLAN Remove

Feb 07 12:48:572013: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to wlan
ICSA-testing is getting altered.

MAC ACL OUT on WLAN Attach

Feb 07 12:49:00 2013: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to wlan
ICSA-testing is getting altered.

MAC ACL OUT on WLAN Remove

Feb 07 12:49:06 2013: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to wlan
ICSA-testing is getting altered.

IP ACL on VLAN Attach

Feb 07 12:49:10 201: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to interface vlan1 is getting altered.

IP ACL on VLAN Remove

Feb 07 12:49:12 2013: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to interface vlan1 is getting altered.

IP ACL on GE Port Attach

Feb 07 12:49:15 2013: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to interface ge1 is getting altered.

IP ACL on GE Port Remove

Feb 07 12:49:20 2013: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to interface ge1 is getting altered.

MAC ACL on GE Port Attach

Feb 07 12:49:22 2013: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to interface ge1 is getting altered.

MAC ACL on GE Port Remove

Feb 07 12:49:24 2013: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to interface ge1 is getting altered.

IP ACL on Port-Channel Attach

Feb 07 12:49:30 2013: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to interface
port-channel1 is getting altered.

IP ACL on Port-Channel Remove

Feb 07 12:50:00 2013: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to interface
port-channel1 is getting altered.

MAC ACL on Port-Channel Attach

Feb 07 12:50:01 2013: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to interface
port-channel1 is getting altered.

MAC ACL on Port-Channel Remove

Feb 07 12:50:05 2013: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to interface
port-channel1 is getting altered.

Rule added / deleted from IP/MAC ACL

Feb 26 20:32:56 2013: %CFGD-6-ACL_RULE_ALTERED: USER: admin session 3: ACL foo rule is getting altered.

TCP Reset Packets log

For any change in the TCP configuration, a TCP reset log is generated. The following example displays the initial TCP packets permitted before the session timedout:

Feb 07 20:31:26 2013: %DATAPLANE-5-LOGRULEHIT: Matched ACL:ftpuser:ip Rule:1 Disposition:Allow Packet Src MAC:<00-19-B9-6B-DA-77> Dst MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.1.99 Dst IP:192.168.2.102 Proto:6 Src Port:3318 Dst Port:21.

Feb 07 20:31:31 2013: %DATAPLANE-5-LOGRULEHIT: Matched ACL:ftpuser:ip Rule:1 Disposition:Allow Packet Src MAC:<00-19-B9-6B-DA-77> Dst MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.1.99 Dst IP:192.168.2.102 Proto:6 Src Port:3318 Dst Port:21.

ICMP Destination log

The following example displays an ICMP destination as unreachable when no matching payload is found:

Feb 07 19:57:09 2013: %DATAPLANE-5-ICMPPKTDROP: Dropping ICMP Packet from 192.168.1.104 to 192.168.2.102, with ProtocolNumber:1 ICMP code 3 and ICMP type 3. Reason: no flow matching payload of ICMP Error.

Feb 07 19:57:09 2013: %DATAPLANE-5-ICMPPKTDROP: Dropping ICMP Packet from 192.168.1.104 to 192.168.2.102, with ProtocolNumber:1 ICMP code 3 and ICMP type 3. Reason: no flow matching payload of ICMP Error.

To generate an ICMP protocol log, an ACL rule has to be applied and logging has to be enabled.

For example, the following command has to be executed:

```
rfs7000-37FABE(config-ip-acl-test)#permit icmp any any log rule-precedence 20
rfs7000-37FABE(config-ip-acl-test)#
```

ICMP Packet log

Feb 07 20:37:04 2013: %DATAPLANE-5-LOGRULEHIT: Matched ACL:ftpuser:ip Rule:0 Disposition:Drop Packet Src MAC:<00-19-B9-6B-DA-77> Dst MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.1.99 Dst IP:192.168.1.1 Proto:1 ICMP Type:8 ICMP Code:0.

Feb 07 20:37:08 2013: %DATAPLANE-5-ICMPPKTDROP: Dropping ICMP Packet from 192.168.2.1 to 172.16.31.196, with Protocol Number:1 ICMP code 3 and ICMP type 3. Reason: no flow matching payload of ICMP Error.

To generate an ICMP protocol log, an ACL rule has to be applied and logging has to be enabled:

For example, the following command has to be executed:

```
rfs7000-37FABE(config-ip-acl-test)#permit icmp any any log rule-precedence 20
rfs7000-37FABE(config-ip-acl-test)#
```

SSH connection log

A SSH connection is enabled on the wireless controller using factory settings.

Running primary software, version 5.5.0.0-149320X

Alternate software secondary, version 5.4.0.0-048D

Software fallback feature is enabled

System bootup time (via /proc/uptime) was 126.10 92.38

Please press Enter to activate this console. Feb 07 20:47:33 2013: %DOT11-5-COUNTRY_CODE: Country of operation configured to in [India]

Feb 07 20:47:34 2013: %DIAG-6-NEW_LED_STATE: LED state message AP_LEDS_ON from module DOT11

Feb 07 20:47:34 2013: KERN: vlan1: add 01:00:5e:00:00:01 mcast address to master interface.

Feb 07 20:47:34 2013: %NSM-4-IFUP: Interface vlan2 is up

Feb 07 20:47:34 2013: KERN: vlan2: add 01:00:5e:00:00:01 mcast address to master interface.

Feb 07 20:47:34 2013: %NSM-4-IFUP: Interface vlan172 is up

Feb 07 20:47:34 2013: KERN: vlan172: add 01:00:5e:00:00:01 mcast address to master interface.

Feb 07 20:47:34 2013: %DAEMON-3-ERR: dhcrelay: interface allocate: vlan1

Feb 07 20:47:34 2013: %PM-6-PROCSTART: Starting process "/usr/sbin/sshd"

Feb 07 20:47:34 2013: %DAEMON-3-ERR: dhcrelay: idataplane enabled

Interface allocatCCB:21:Firewall enabled

Interface : vlan1

Feb 07 20:47:34 2013: %DAEMON-3-ERR: dhcrelay: interface allocate : vlan2

Feb 07 20:47:34 2013: %KERN-4-WARNING: dataplane enabled.

Feb 07 20:47:34 2013: %DATAPLANE-5-FWSTARTUP: Firewall enabled.

Feb 07 20:47:39 2013: %DATAPLANE-5-LOGRULEHIT: Matched ACL:ftpuser:ip Rule:0 Disposition:Drop Packet Src MAC:<00-19-B9-6B-DA-77> Dst MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.1.99 Dst IP:192.168.1.1 Proto:6 Src Port:3327 DstPort:22.

Allowed/Dropped Packets Log

The following example displays disposition information regarding allow/deny packets:

Allow Packets

CCB:0:Matched ACL:ftpuser:ip Rule:1 Disposition:Allow Packet Src MAC:<00-11-25-14-D9-E2> Dst MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.2.102 Dst IP:192.168.2.1 Proto:17 Src Port:137 Dst Port:137

CCB:0:Matched ACL:ftpuser:ip Rule:1 Disposition:**Allow** Packet Src MAC:<00-11-25-14-D9-E2> Dst MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.2.102 Dst IP:192.168.2.1 Proto:17 Src Port:1029 Dst Port:53

CCB:Feb 07 18:14:32 2013: %DATAPLAN:-5-LOGRULEHIT: Matched ACL:ftpuer:aip Rule:1 Ditcposition:Allow hedacket Src MAC: 00-11-25-14-D9-A2> Dst MAC:<00-5-70-81-9C1-6A> thertLype:0x0800:Src IP:192.168..102 Dsft IP:192t168.2.1 Proto:1p Src Port:137 Dut Port:137.

ser:ip Rule:1 Disposition:Allow Packet Src MAC:<00-11-25-14-D9-E2> Dst MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.2.102 Dst IP:192.168.2.1 Proto:17 Src Port:1029 Dst Port:53

Drop/Deny Packets

CCB:0:Matched ACL:ftpuser:ip Rule:0 Disposition:**Drop** Packet Src MAC:<00-11-25-14-D9-E2> Dst MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.2.102 Dst IP:192.168.2.1 Proto:17 Src Port:137 Dst Port:137

Feb 07 20:41:28 2013: %DATAPLANE-5-LOGRULEHIT: Matched ACL:ftpuser:ip Rule:0 Disposition:Drop Packet Src MAC:<00-11-25-14-D9-E2> Dst MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.2.102 Dst IP:192.168.2.1 Proto:17 Src Port:137 Dst

To generate an allow/deny protocol log, an ACL rule has to be applied and logging has to be enabled.

For example, the following commands have to be executed:

```
rfs7000-37FABE(config-ip-acl-test)#permit ip any any log rule-precedence 20
rfs7000-37FABE(config-ip-acl-test)#
rfs7000-37FABE(config-ip-acl-test)#deny ip any any log rule-precedence 20
rfs7000-37FABE(config-ip-acl-test)#
```

Appendix

CONTROLLER MANAGED WLAN USE CASE A

This section describes the activities required to configure a WLAN. Instructions are provided using the wireless controller CLI.

Creating a First Controller Managed WLAN

CONTROLLER MANAGED WLAN USE CASE

It is assumed you have a Brocade Mobility RFS4000 wireless controller with the latest build available from Brocade. It is also assumed you have one Brocade Mobility 650 Access Point model access point and one Brocade Mobility 71XX Access Point model access point, both with the latest firmware available from Brocade.

Upon completion, you will have created a WLAN on a Brocade Mobility RFS4000 model wireless controller using a DHCP server to allocate IP addresses to associated wireless clients.

Assumptions

Verify the following conditions have been satisfied before attempting the WLAN configuration activities described in this section:

- It is assumed the wireless controller has the latest firmware version available from Brocade.
- It is assumed the Brocade Mobility 650 Access Point and Brocade Mobility 71XX Access Point access points also have the latest firmware version available from Brocade.
- It is assumed there are no previous configurations on the wireless controller or access point and default factory configurations are running on the devices.
- It is assumed you have administrative access to the wireless controller and access point CLI.
- It is assumed the individual administrating the network is a professional network installer.

Design

This section defines the network design being implemented.

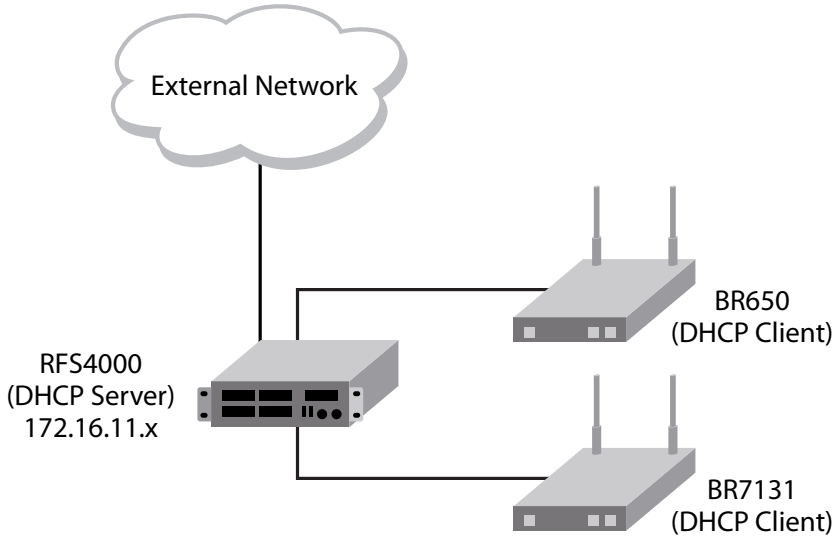


FIGURE 1 Network Design

This is a simple deployment scenario, with the access points connected directly to the wireless controller. One wireless controller port is connected to an external network.

On the Brocade Mobility RFS4000 wireless controller, the GE1 interface is connected to an external network. Interfaces GE3 and GE4 are used by the access points.

On the external network, the wireless controller is assigned an IP address of 192.168.10.188. The wireless controller acts as a DHCP server for the wireless clients connecting to it, and assigns IP addresses in the range of 172.16.11.11 to 172.16.11.200. The rest of IPs in the range are reserved for devices requiring static IP addresses.

Using the Command Line Interface to Configure the WLAN

Creating a First Controller Managed WLAN

These instructions are for configuring your first WLAN using the wireless controller CLI.

Use a serial console cable when connecting to the wireless controller for the first time. Set the following configuration when using the serial connection:

- Bits per second:*19200*
- Data Bit**:** *8*
- Parity**:** *None*
- Stop Bit: *1*
- Flow Control: *None*

The steps involved in creating a WLAN on a wireless controller are:

Logging Into the Controller for the First Time

Creating a RF Domain

Creating a Wireless Controller Profile

Creating an AP Profile

Creating a DHCP Server Policy

Completing and Testing the Configuration

Logging Into the Controller for the First Time

Using the Command Line Interface to Configure the WLAN

When powering on the wireless controller for the first time, you are prompted to replace the existing administrative password. The credentials for logging into the wireless controller for the first time are:

- User Name: *admin*
- Password: *admin123*

Ensure the new password created is strong enough to provide adequate security for the wireless controller managed network.

Creating a RF Domain

Using the Command Line Interface to Configure the WLAN

A RF Domain is a collection of configuration settings specific to devices located at the same physical deployment, such as a building or a floor. Create a RF Domain and assign the country code where the devices are deployed. This is a mandatory step, and the devices will not function as intended if this step is omitted.

The instructions in this section must be performed from the Global Configuration mode of the wireless controller. To navigate to this mode:

```
rfs4000>enable
rfs4000#
rfs4000#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
rfs4000(config)#
```

Create the RF Domain using the following commands:

```
rfs4000(config)#rf-domain RFDOMAIN_UseCase1
rfs4000(config-rf-domain-RFDOMAIN_UseCase1)#
```

This command creates a profile with the name *RFDOMAIN_UseCase1*.

Set the country code for the RF Domain.

```
rfs4000(config-rf-domain-RFDOMAIN_UseCase1)#country-code us
```

This sets the country code for this RF Domain. Save this change and exit the RF Domain profile context.

```
rfs4000(config-rf-domain-RFDOMAIN_UseCase1)#commit write
rfs4000(config-rf-domain-RFDOMAIN_UseCase1)#exit
rfs4000(config)#
```

To define the wireless controller's physical location, use the same RF Domain configuration.

```
rfs4000(config)#self
rfs4000(config-device-03-14-28-57-14-28)#
rfs4000(config-device-03-14-28-57-14-28)#use rf-domain RFDOMAIN_UseCase1
```

Commit the changes and write to the running configuration. Exit this context.

```
rfs4000(config-device-03-14-28-57-14-28)#commit write
rfs4000(config-device-03-14-28-57-14-28)#exit
rfs4000(config)#
```

Creating a Wireless Controller Profile

Using the Command Line Interface to Configure the WLAN

The first step in creating a WLAN is to configure a profile defining the parameters applied to a wireless controller.

To create a profile:

```
rfs4000(config)#profile rfs4000 Brocade Mobility RFS4000_UseCase1
rfs4000(config-profile-Brocade Mobility RFS4000_UseCase1)#
```

This creates a profile with the name *Brocade Mobility RFS4000_UseCase1* and moves the cursor into its context. Any configuration made under this profile is available when it is applied to a device.

Configure a VLAN

Create the VLAN to use with the WLAN configuration. This can be done using the following commands:

```
rfs4000(config-profile-Brocade Mobility RFS4000_UseCase1)#interface vlan 2
rfs4000(config-profile-Brocade Mobility RFS4000_UseCase1-if-vlan2)#ip address
172.16.11.1/24
```

The above command assigns the IP address 172.16.11.1 with the mask of 255.255.255.0 to VLAN 2. Exit the VLAN 2 context.

```
rfs4000(config-profile-Brocade Mobility RFS4000_UseCase1-if-vlan2)#exit
rfs4000(config-profile-Brocade Mobility RFS4000_UseCase1)#
```

The next step is to assign this newly created VLAN to a physical interface. In this case, VLAN 2 is mapped to GE3 and GE4 to support two access points, an Brocade Mobility 650 Access Point and an Brocade Mobility 71XX Access Point. The Brocade Mobility 650 Access Point is connected to the gigabit interface GE3 and the Brocade Mobility 71XX Access Point to the GE4 interface.

```
rfs4000(config-profile-Brocade Mobility RFS4000_UseCase1)#interface ge 3
rfs4000(config-profile-Brocade Mobility RFS4000_UseCase1-if-ge3)#
```

Map VLAN 2 to this interface. This assigns the IP address to the selected physical interface.

```
rfs4000(config-profile-Brocade Mobility RFS4000_UseCase1-if-ge3)#switchport
access vlan 2
rfs4000(config-profile-Brocade Mobility RFS4000_UseCase1-if-ge3)#exit
rfs4000(config-profile-Brocade Mobility RFS4000_UseCase1)#
```

Similarly, map the defined VLAN 2 to the GE4 interface.

```
rfs4000(config-profile-1_UseCase1)#interface ge 4
rfs4000(config-profile-Brocade Mobility RFS4000_UseCase1-if-ge4)#switchport
access vlan 2
rfs4000(config-profile-Brocade Mobility RFS4000_UseCase1-if-ge4)#exit
rfs4000(config-profile-Brocade Mobility RFS4000_UseCase1)#
```

Exit the profile and save it.

```
rfs4000(config-profile-Brocade Mobility RFS4000_UseCase1)#exit
rfs4000(config)#commit write
```

Configure the Wireless Controller to use the Profile

Before the wireless controller can be further configured, the profile must be applied to the wireless controller.

```
rfs4000(config)#self
rfs4000(config-device-03-14-28-57-14-28)#
rfs4000(config-device-03-14-28-57-14-28)#use profile Brocade Mobility
RFS4000_UseCase1
rfs4000(config-device-03-14-28-57-14-28)#exit
rfs4000(config)#commit write
```

Create a WLAN

Use the following commands to create a WLAN:

```
rfs4000(config)#wlan 1
rfs4000(config-wlan-1)#
```

Configure the SSID for the WLAN. This is the value that identifies and helps differentiate this WLAN.

```
rfs4000(config-wlan-1)#ssid WLAN_USECASE_01
```

Enable the SSID to be broadcast so wireless clients can find it and associate.

```
rfs4000(config-wlan-1)#broadcast-ssid
```

Associate VLAN 2 to the WLAN and exit.

```
rfs4000(config-wlan-1)#vlan 2
rfs4000(config-wlan-1)#exit
```

Commit the Changes

Once these changes have been made, they have to be committed before proceeding.

```
rfs4000(config)#commit write
```

Creating an AP Profile

Using the Command Line Interface to Configure the WLAN

An AP profile provides a method of applying common settings to access points of the same model. The profile significantly reduces the time required to configure access points within a large deployment. For more information, see:

- *Creating a Brocade Mobility 650 Access Point Profile*
- *Creating a Brocade Mobility 71XX Access Point Profile*

Creating a Brocade Mobility 650 Access Point Profile

Creating an AP Profile

A Brocade Mobility 650 Access Point's firmware is updated directly by its associated wireless controller. The process is automatic, and no intervention is required. To create a profile for use with an Brocade Mobility 650 Access Point:

```
rfs4000(config)#profile br650 Brocade Mobility 650 Access Point_UseCase1
rfs4000(config-profile-Brocade Mobility 650 Access Point_UseCase1)#
```

Assign the access point to be a member of the same VLAN defined in "Creating an AP Profile" on page 1343. In this section, the VLAN was defined as VLAN 2. Configure the access point to be a member of VLAN 2.

```
rfs4000(config-profile-AP650_UseCase1)#interface vlan 2
rfs4000(config-profile-AP650_UseCase1-if-vlan2)#
```

Configure this VLAN to use DHCP, so any device that is associated using this access point is automatically assigned a unique IP address. Once completed, exit this context.

```
rfs4000(config-profile-Brocade Mobility 650 Access Point_UseCase1-if-vlan2)#ip
address dhcp
rfs4000(config-profile-Brocade Mobility 650 Access
Point_UseCase1-if-vlan2)#exit
```

The VLAN has to be mapped to a physical interface on the access point. Since the only available physical interface on the Brocade Mobility 650 Access Point is GE1, this VLAN is mapped to it.

```
rfs4000(config-profile-Brocade Mobility 650 Access Point_UseCase1)#interface
ge 1
rfs4000(config-profile-Brocade Mobility 650 Access
Point_UseCase1-if-ge1)#switchport access vlan 2
rfs4000(config-profile-Brocade Mobility 650 Access Point_UseCase1-if-ge1)#exit
```

Before a WLAN can be implemented, it has to be mapped to a radio on the access point. An Brocade Mobility 650 Access Point has 2 radios, in this scenario, both radios are utilized.

```
rfs4000(config-profile-Brocade Mobility 650 Access Point_UseCase1)#interface
radio 1
rfs4000(config-profile-Brocade Mobility 650 Access
Point_UseCase1-if-radio1)#wlan 1
rfs4000(config-profile-Brocade Mobility 650 Access
Point_UseCase1-if-radio1)#exit
rfs4000(config-profile-Brocade Mobility 650 Access Point_UseCase1)#interface
radio 2
rfs4000(config-profile-Brocade Mobility 650 Access
Point_UseCase1-if-radio2)#wlan 1
rfs4000(config-profile-Brocade Mobility 650 Access
Point_UseCase1-if-radio2)#exit
rfs4000(config-profile-Brocade Mobility 650 Access Point_UseCase1)#
```

Commit the changes made to this profile and exit.

```
rfs4000(config-profile-Brocade Mobility 650 Access Point_UseCase1)#commit
write
rfs4000(config-profile-Brocade Mobility 650 Access Point_UseCase1)#exit
rfs4000(config)#
```

Apply this Profile to the Discovered Brocade Mobility 650 Access Point

Access the discovered access point using the following command. The discovered device's MAC address is used to access its context.

```
rfs4000(config)#br650 00-A0-F8-00-00-01
rfs4000(config-device-00-A0-F8-00-00-01)#
```

Assign the AP profile to this Brocade Mobility 650 Access Point access point.

```
rfs4000(config-device-00-A0-F8-00-00-01)#use profile AP650_UseCase1
rfs4000(config-device-00-A0-F8-00-00-01)#commit write
```

Apply the RF Domain profile to the AP

Apply the previously created RF Domain to enable a country code to be assigned to the discovered access point. A discovered access point only works properly if its country code is the country code of its associated wireless controller.

```
rfs4000(config-device-00-A0-F8-00-00-01)#use rf-domain RFDOMAIN_UseCase1
rfs4000(config-device-00-A0-F8-00-00-01)#commit write
rfs4000(config-device-00-A0-F8-00-00-01)#exit
rfs4000(config)#
```

Creating a Brocade Mobility 71XX Access Point Profile

Creating an AP Profile

To create a profile for use with an Brocade Mobility 71XX Access Point:

```
rfs4000(config)#profile br7131 Brocade Mobility 7131 Access Point_UseCase1
rfs4000(config-profile-Brocade Mobility 7131 Access Point_UseCase1)#
```

Set the access point to be a member of the same VLAN defined in "Creating an AP Profile" on page 1343. In this section, the VLAN was defined as VLAN 2. Configure the access point to be a member of the VLAN 2.

```
rfs4000(config-profile-Brocade Mobility 7131 Access Point_UseCase1)#interface
vlan 2
rfs4000(config-profile-Brocade Mobility 7131 Access Point_UseCase1-if-vlan2)#
```

Configure this VLAN to use DHCP, so any device associated using this access point is automatically assigned a unique IP address. Once completed, exit this context.

```
rfs4000(config-profile-Brocade Mobility 7131 Access
Point_UseCase1-if-vlan2)#ip address dhcp
rfs4000(config-profile-Brocade Mobility 7131 Access
Point_UseCase1-if-vlan2)#exit
```

The configured VLAN has to be mapped to a physical interface on the access point. Map VLAN 2 to the GE1 and GE2 interfaces on the Brocade Mobility 71XX Access Point. To configure the GE1 interface:

```
rfs4000(config-profile-Brocade Mobility 7131 Access Point_UseCase1)#interface
ge 1
rfs4000(config-profile-Brocade Mobility 7131 Access
Point_UseCase1-if-ge1)#switchport access vlan 2
rfs4000(config-profile-Brocade Mobility 7131 Access
Point_UseCase1-if-ge1)#exit
```

Similarly configure the GE2 interface.

```
rfs4000(config-profile-Brocade Mobility 7131 Access Point_UseCase1)#interface
ge 2
rfs4000(config-profile-Brocade Mobility 7131 Access
Point_UseCase1-if-ge2)#switchport access vlan 2
rfs4000(config-profile-Brocade Mobility 7131 Access
Point_UseCase1-if-ge2)#exit
```

Before the WLAN can be implemented, it has to be mapped to the physical radio on the access point. An Brocade Mobility 71XX Access Point has 3 radios (on certain models), two of which can be configured for WLAN support. In this scenario, two radios are used.

```
rfs4000(config-profile-Brocade Mobility 7131 Access Point_UseCase1)#interface
radio 1
rfs4000(config-profile-Brocade Mobility 7131 Access
Point_UseCase1-if-radio1)#wlan 1
rfs4000(config-profile-Brocade Mobility 7131 Access
Point_UseCase1-if-radio1)#exit
rfs4000(config-profile-Brocade Mobility 7131 Access Point_UseCase1)#interface
radio 2
```

```
rfs4000(config-profile-Brocade Mobility 7131 Access
Point_UseCase1-if-radio2)#wlan 1
rfs4000(config-profile-Brocade Mobility 7131 Access
Point_UseCase1-if-radio2)#exit
rfs4000(config-profile-Brocade Mobility 7131 Access Point_UseCase1)#
```

Commit the changes made to the profile and exit this context.

```
rfs4000(config-profile-Brocade Mobility 7131 Access Point_UseCase1)#commit
write
rfs4000(config-profile-Brocade Mobility 7131 Access Point_UseCase1)#exit
rfs4000(config)#
```

Apply this Profile to the Discovered Brocade Mobility 71XX Access Point

Access the discovered access point using the following command. The discovered device's MAC address is used to access its context.

```
rfs4000(config)#br7131 00-23-68-16-C6-C4
rfs4000(config-device-00-23-68-16-C6-C4)#
```

Assign the AP profile to this access point.

```
rfs4000(config-device-00-23-68-16-C6-C4)#use profile AP7131_UseCase1
rfs4000(config-device-00-23-68-16-C6-C4)#commit write
```

Apply the RF Domain profile to the AP

Apply the previously created RF Domain to enable a country code to be assigned to the discovered access point. A discovered access point only works properly if its country code is the same as its associated wireless controller.

```
rfs4000(config-device-00-23-68-16-C6-C4)#use rf-domain RFDOMAIN_UseCase1
rfs4000(config-device-00-23-68-16-C6-C4)#commit write
rfs4000(config-device-00-23-68-16-C6-C4)#Exit
rfs4000(config)#
```

Creating a DHCP Server Policy

Using the Command Line Interface to Configure the WLAN

The DHCP server policy defines the parameters required to run a DHCP server on the wireless controller and assign IP addresses automatically to devices that associate. Configuring DHCP enables the reuse of a limited set of IP addresses.

To create a DHCP server policy:

```
rfs4000-37FABE(config)#dhcp-server-policy DHCP_POLICY_UseCase1
rfs4000-37FABE(config-dhcp-policy-DHCP_POLICY_UseCase1)#
```

Table 1 displays how IP addresses are used.

TABLE 1 IP Address Usage

IP Range	Usage
172.16.11.1 till 172.16.11.10	Reserved for devices that require a static IP address
172.16.11.11 till 172.16.11.200	Range of IP addresses that can be assigned using the DHCP server.
172.16.11.201 till 172.16.11.254	Reserved for devices that require a static IP address

In the table, the IP address range of 172.16.11.11 to 172.16.11.200 is available using the DHCP server. To configure the DHCP server:

```
rfs4000-37FABE(config-dhcp-policy-DHCP_POLICY_UseCase1)#dhcp-pool
DHCP_POOL_USECASE1_01
rfs4000-37FABE(config-dhcp-policy-DHCP_POLICY_UseCase1-pool-DHCP_POOL_USECASE
1_01)#
```

Configure the address range as follows:

```
rfs4000-37FABE(config-dhcp-policy-DHCP_POLICY_UseCase1-pool-DHCP_POOL_USECASE
1_01)#address range 172.16.11.11 172.16.11.200
rfs4000-37FABE(config-dhcp-policy-DHCP_POLICY_UseCase1-pool-DHCP_POOL_USECASE
1_01)#
```

Configure the IP pool used with a network segment. This starts the DHCP server on the specified interface.

```
rfs4000-37FABE(config-dhcp-policy-DHCP_POLICY_UseCase1-pool-DHCP_POOL_USECASE
1_01)#network 172.16.11.0/24
rfs4000-37FABE(config-dhcp-policy-DHCP_POLICY_UseCase1-pool-DHCP_POOL_USECASE
1_01)#exit
rfs4000-37FABE(config-dhcp-policy-DHCP_POLICY_UseCase1)#exit
rfs4000-37FABE(config)#commit write
```

Configure the Brocade Mobility RFS4000 to use the DHCP Policy

For the DHCP to work properly, the new DHCP Server Policy must be applied to the wireless controller. To apply the DHCP Server Policy to the wireless controller:

```
rfs4000-37FABE(config)#self
rfs4000-37FABE(config-device-03-14-28-57-14-28)#use dhcp-server-policy
DHCP_POLICY_UseCase1
rfs4000-37FABE(config-device-03-14-28-57-14-28)#commit write
rfs4000-37FABE(config-device-03-14-28-57-14-28)#exit
rfs4000-37FABE(config)#
```

Completing and Testing the Configuration

Using the Command Line Interface to Configure the WLAN

A wireless client must be configured to associate with the wireless controller managed WLAN. The following information must be defined:

- SSID: WLAN_USECASE_01
- Country: Same as the country configured in *Creating a RF Domain on page A-1341*. In this scenario, the country code is set to US.
- Mode: Infrastructure

With the WLAN set to beacon, use the wireless client's discovery client to discover the configured WLAN and associate.