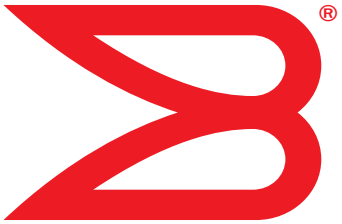
53-1002740-01
29 November 2012



Brocade Mobility RFS4000, RFS6000, and RFS7000

CLI Reference Guide

Supporting software release 5.4.0.0 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 RFS4000, RFS6000, and RFS7000 CLI Reference Guide	53-1002313-01	New document	June 2011
Brocade Mobility RFS4000, RFS6000, and RFS7000 CLI Reference Guide	53-1002486-01	New Additions for software version 5.2.0.0	November 2011
Brocade Mobility RFS4000, RFS6000, and RFS7000 CLI Reference Guide	53-1002619-01	New Additions for software version 5.3.0.0	May 2012
Brocade Mobility RFS4000, RFS6000, and RFS7000 CLI Reference Guide	53-1002740-01	New Additions for software version 5.4.0.0	November 2012

Contents

Chapter 4 Global Configuration Commands

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 71XX Series Access Point
- Brocade Mobility 300 Access Point
- Brocade Mobility 650 Access Point
- Brocade Mobility 6511 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 RFS4000, RFS6000 and RFS7000 System Reference Guide* - Describes configuration of the Brocade wireless controllers using the Web UI.
- *Brocade Mobility RFS4000, RFS6000 and RFS7000 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

1 Introduction

In this chapter

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

Access the CLI by using:

- A terminal emulation program running on a computer connected to the serial port on the wireless controller. The serial port is located on the front of the wireless controller.
- A Telnet session through *Secure Shell* (SSH) over a network.

Configuration for connecting to a Wireless 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 the each supported wireless controller model and AP. 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.

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 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.

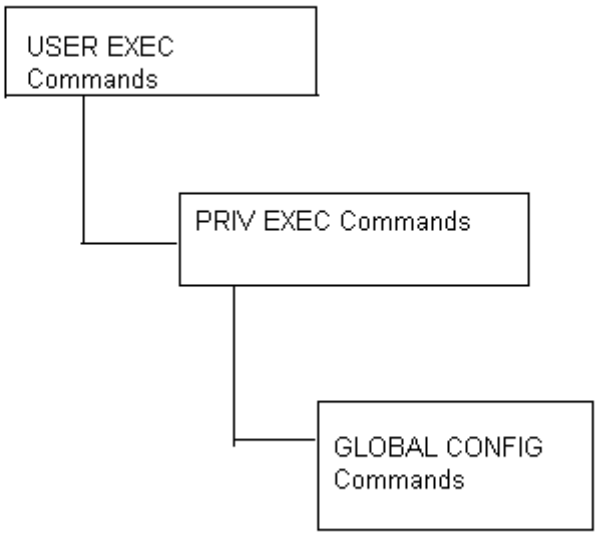


FIGURE 1 Hierarchy of User Modes

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 wireless controller 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 wireless controller 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 wireless controller 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 wireless controller commands.

TABLE 1 Wireless Controller Modes and Commands

User Exec Mode	Priv Exec Mode	Global Configuration Mode
ap-upgrade	ap-upgrade	aaa-policy
captive-portal-page-upload	archive	aaa-tacacs-policy
change-passwd	boot	advanced-wips-policy
clear	captive-portal-page-upload	br300
commit	clear	br650
connect	clock	br6511
disable	connect	br71xx
enable	copy	association-acl-policy
help	create-cluster	auto-provisioning-policy
join-cluster	crypto	captive-portal
l2tpv3	debug	clear
logging	delete	customize
mint	diff	device
no	dir	device-categorization
page	disable	dhcp-server-policy
ping	edit	dns-whitelist

TABLE 1 Wireless Controller Modes and Commands

User Exec Mode	Priv Exec Mode	Global Configuration Mode
revert	enable	event-system-policy
service	erase	firewall-policy
show	format	help
ssh	halt	host
telnet	help	igmp-snoop-policy
terminal	join-cluster	inline-password-encryption
time-it	l2tpv3	ip
traceroute	logging	l2tpv3
watch	mint	mac
write	mkdir	management-policy
clrscr	more	meshpoint
exit	no	meshpoint-qos-policy
	page	mint-policy
	ping	nac-list
	pwd	no
	re-elect	password-encryption
	reload	profile
	remote-debug	radio-qos-policy
	rename	radius-group
	revert	radius-server-policy
	rmdir	radius-user-pool-policy
	self	rf-domain
	service	rfs4000
	show	rfs6000
	ssh	rfs7000
	terminal	role-policy
	time-it	routing-policy
	traceroute	self
	upgrade	smart-rf-policy
	upgrade-abort	wips-policy
	watch	wlan
	write	wlan-qos-policy
	clrscr	write
	exit	clrscr
		commit
		do

TABLE 1 Wireless Controller Modes and Commands

User Exec Mode	Priv Exec Mode	Global Configuration Mode
		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
  br300               Set global BRbr300300 parameters
  clear               Remove
  cli-tables-skin     Choose a formatting layout/skin for CLI tabular outputs
  cluster             Cluster Protocol
  delete-offline-aps  Delete Access Points that are configured but offline
  enable              Enable radiusd loading on low memory devices
  force-send-config   Resend configuration to the device
  load-balancing      Wireless load-balancing service commands
  locator             Enable leds flashing on the device
  radio               Radio parameters
  radius              Radius test
  set                 Set validation mode
  show                Show running system information
  smart-rf            Smart-RF Management Commands
  ssm                 Command related to ssm
  wireless            Wireless commands

rfs7000-37FABE>
```

It’s 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 wireless 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

TABLE 2 Keystrokes Details

Keystrokes	Function Summary	Function Details
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# co
```

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 wireless controller profile
- a default profile for each of the following access points:
  - Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point

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
 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 radio3
 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 vlan1
--More--
```

Change the default profile by creating VLAN 150 and mapping to ge3 physical interface

Logon to the wireless 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 ap configured
------------------------------------------------------------------------------
--------
 IDX      NAME             MAC            PROFILE      RF-DOMAIN    ADOPTED-BY
------------------------------------------------------------------------------
--------
  1   br71xx-139B34   00-23-68-13-9B-34   default-br71xx   default
un-adopted
  2   br7131-4AA708   00-04-96-4A-A7-08   default-br71xx   default
un-adopted
  3   br71xx-889EC4   00-15-70-88-9E-C4   default-br71xx   default
un-adopted
  4   br650-000001    00-A0-F8-00-00-01   default-br650    default
un-adopted
  5   br650-000010    00-A0-F8-00-00-10   default-br650    default
un-adopted
  6   br650-311641    00-23-68-31-16-41   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 wireless controller.

- A terminal emulation program running on a computer connected to the serial port on the wireless controller. The serial port is located on the front of the wireless 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 wireless 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 wireless 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 wireless 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
symbol 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 snmpoperator v3 encrypted des auth md5 0 operator
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 wireless controller.

```
rfs7000 release 5.4.0.0-144745X
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 wireless controller. The wireless 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.
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 wireless wireless 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 wireless controller for the first time, you are prompted to change the password.

- To change the user credentials:

```
rfs7000 release 5.4.0.0-144745X
rfs7000-37FABE login: testuser
Password:
Welcome to CLI
Starting CLI...
rfs7000-37FABE>
```

Chapter

2 User Exec Mode Commands

In this chapter

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 (>).

```
rfs7000-37FABE>?
Command commands:
  ap-upgrade                  AP firmware upgrade
  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
  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
  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
  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
rfs7000-37FABE>
```

User Exec Commands

Table 1 summarizes User Exec Mode commands.

TABLE 1 User Exec Mode Commands

Command	Description	Reference
ap-upgrade	Enables an automatic adopted AP firmware upgrade	*page 2-15*
captive-portal-page-upload	Uploads captive portal advanced pages	*page 2-20*
change-passwd	Changes the password of a logged user	*page 2-22*
clear	Resets the last saved command	*page 2-22*
clock	Configures the system clock	*page 2-26*
cluster	Accesses the cluster context	*page 2-27*
connect	Establishes a console connection to a remote device	*page 2-28*
create-cluster	Creates a new cluster on a specified device	*page 2-29*
crypto	Enables encryption	*page 2-29*
disable	Turns off (disables) the privileged mode command set	*page 2-39*
enable	Turns on (enables) the privileged mode command set	*page 2-39*
join-cluster	Adds a wireless controller to an existing cluster of devices	*page 2-39*
l2tpv3	Establishes or brings down *Layer 2 Tunneling Protocol Version 3* (L2TPV3) tunnel	*page 2-41*
logging	Modifies message logging facilities	*page 2-42*
exit	Ends the current CLI session and closes the session window	*page 2-43*
mint	Configures MiNT protocol	*page 2-43*
no	Negates a command or sets its default	*page 2-45*
page	Toggles to the wireless controller paging function	*page 2-48*
ping	Sends ICMP echo messages to a user-specified location	*page 2-48*
ssh	Opens an SSH connection between two network devices	*page 2-49*
telnet	Opens a Telnet session	*page 2-50*
terminal	Sets the length/number of lines displayed within the terminal window	*page 2-50*
time-it	Verifies the time taken by a particular command between request and response	*page 2-51*
traceroute	Traces the route to its defined destination	*page 2-52*
watch	Repeats a specific CLI command at a periodic interval	*page 2-53*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*

TABLE 1 User Exec Mode Commands

Command	Description	Reference
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes information to memory or terminal	*page 5-310*

ap-upgrade

User Exec Commands

Enables automatic firmware upgrade on an adopted AP or a set of APs. APs of the same type can be upgraded together. Once APs have been upgraded, they can be forced to reboot. This command also loads the firmware on to the wireless controller.

The AP upgrade command also upgrades APs in a specified RF Domain.

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
ap-upgrade [<MAC/HOSTNAME>|all|br650|br6511|br71xx|
           cancel-upgrade|load-image|rf-domain]

ap-upgrade [<MAC/HOSTNAME>] {no-reboot|reboot-time <TIME>|
           upgrade-time <TIME> {no-reboot|reboot-time <TIME>}}

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

ap-upgrade [br650|br6511|br71xx] all
   {no-reboot|reboot-time <TIME>|upgrade-time <TIME> {no-reboot|reboot-time
<TIME>}}
           {(staggered-reboot)}

ap-upgrade cancel-upgrade [<MAC/HOSTNAME>|all|br650|br6511|br71xx|on]
ap-upgrade cancel-upgrade [<MAC/HOSTNAME>|all]
ap-upgrade cancel-upgrade [br650|br6511|br71xx] all
ap-upgrade cancel-upgrade on rf-domain [<RF-DOMAIN-NAME>|all]

ap-upgrade load-image [br650|br6511|br71xx]
           <IMAGE-URL>

ap-upgrade rf-domain [<RF-DOMAIN-NAME>|all] [all|br650|br6511|
           br71xx] {no-reboot|no-via-rf-domain|reboot-time <TIME>|
           staggered-reboot|upgrade-time <TIME>}

ap-upgrade rf-domain [<RF-DOMAIN-NAME>|all] [all|br650|br6511|
           br71xx] {no-reboot {staggered-reboot}|
           reboot-time <TIME> {staggered-reboot}}
```

```
ap-upgrade rf-domain [<RF-DOMAIN-NAME>|all] [all|br650|br6511|
br71xx] {no-via-rf-domain {no-reboot|reboot-time <TIME>|
          upgrade-time <TIME> {no-reboot|reboot-time <TIME>}}}
{(staggered-reboot)}

ap-upgrade rf-domain [<RF-DOMAIN-NAME>|all] [all|br650|br6511|
br71xx] {upgrade-time <TIME> {no-reboot|reboot-time <TIME>}}
          {(staggered-reboot)}
```

Parameters

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

<MAC/HOSTNAME>	Upgrades firmware on a specified AP or all APs adopted by the wireless controller • <MAC/HOSTNAME> – Specify the AP's MAC address or hostname.
no-reboot	Optional. Disables automatic reboot after a successful upgrade (the wireless controller 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 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 wireless controller 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.

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

all	Upgrades firmware on all APs adopted by the wireless controller
no-reboot	Optional. Disables automatic reboot after a successful upgrade (the wireless controller 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 firmware upgrade on all adopted APs • <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 wireless controller 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

	`ap-upgrade [br650|br71xx] all {no-reboot|reboot-time <TIME>|upgrade-time <TIME> {no-reboot|reboot-time <TIME>}} {(staggered-reboot)}`
[br650|br6511|br71xx] all	Upgrades firmware on all adopted APs • 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 71XX Access Point all – Upgrades firmware on all Brocade Mobility 71XX Access Points After selecting the AP type, you can schedule an automatic upgrade and/or an automatic reboot.
no-reboot	Optional. Disables automatic reboot after a successful upgrade (the wireless controller 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 firmware upgrade on an AP adopted by the wireless controller • <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 wireless controller 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
	`ap-upgrade cancel-upgrade [<MAC/HOSTNAME>|all]`
cancel-upgrade [<MAC/HOSTNAME>| all]	Cancels a scheduled firmware upgrade on a specified AP or all APs adopted by the wireless controller • <MAC/HOSTNAME> – Cancels a scheduled upgrade on a specified AP. Specify the AP's MAC address or hostname. • all – Cancels scheduled upgrade on all APs
	`ap-upgrade cancel-upgrade [br650|br71xx] all`
cancel-upgrade [br650|br6511| br71xx] all	Cancels scheduled firmware upgrade on all adopted APs • 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 71XX Access Point all – Cancels scheduled upgrade on all Brocade Mobility 71XX Access Points
	`ap-upgrade cancel-upgrade on rf-domain [<DOMAIN-NAME>|all]`
cancel-upgrade on rf-domain [<RF-DOMAIN-NAME>| all]	Cancels scheduled firmware upgrade on a specified RF Domain or all RF Domains • <RF-DOMAIN-NAME> – Cancels scheduled upgrade on a specified RF Domain. Specify the RF Domain name. • all – Cancels scheduled upgrades on all RF Domains

`ap-upgrade load-image [br650|br6511|br71xx] <IMAGE-URL>`

load-image [br650|br6511|br71xx]	Loads AP firmware images on the wireless controller. Select the AP type and provide the location of the AP 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
<IMAGE-URL>	Specify the AP 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

`ap-upgrade rf-domain [<RF-DOMAIN-NAME>|all] [all|br650|br6511|br71xx] {no-reboot {staggered-reboot}|reboot-time <TIME> {staggered-reboot}}`

rf-domain [<RF-DOMAIN-NAME>|all]	Upgrades AP firmware on devices in a specified RF Domain or all RF Domains • <RF-DOMAIN-NAME> – Upgrades firmware in a specified RF Domain. Specify the RF Domain name. • all – Upgrades firmware on all RF Domains
[all|br650|br6511|br71xx]	After specifying the RF Domain, select the AP type. • all – Upgrades firmware on all APs • 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 71XX Access Point – Upgrades firmware on all Brocade Mobility 71XX Access Points
no-reboot {staggered-reboot}	Optional. Disables automatic reboot after a successful upgrade (the wireless controller must be manually restarted) • no-reboot – Optional. Disables automatic reboot after a successful upgrade (the wireless controller 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

`ap-upgrade rf-domain [<RF-DOMAIN-NAME>|all] [all|br650|br6511|br71xx] {no-via-rf-domain {no-reboot|reboot-time <TIME>|upgrade-time <TIME> {no-reboot|reboot-time <TIME>}} {(staggered-reboot)}`

rf-domain [<RF-DOMAIN-NAME>|all]	Upgrades AP firmware on devices in a specified RF Domain or all RF Domains • <RF-DOMAIN-NAME> – Upgrades firmware in a specified RF Domain. Specify the RF Domain name. • all – Upgrades firmware on all RF Domains
[all|br650|br6511|br71xx]	After specifying the RF Domain, select the AP type. • all – Upgrades firmware on all APs • 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 71XX Access Point – Upgrades firmware on all Brocade Mobility 71XX Access Points
no-via-rf-domain	Upgrades APs from the adopted device

no-reboot {staggered-reboot}	Optional. Disables automatic reboot after a successful upgrade (the wireless controller must be manually restarted) • no-reboot – Optional. Disables automatic reboot after a successful upgrade (the wireless controller 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 wireless controller 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

`ap-upgrade rf-domain [<RF-DOMAIN-NAME>|all] [all|br650|br6511|br71xx] {upgrade-time <TIME> {no-reboot|reboot-time <TIME>}} {(staggered-reboot)}`

rf-domain [<RF-DOMAIN-NAME>| all]	Upgrades AP firmware on devices in a specified RF Domain or all RF Domains • <RF-DOMAIN-NAME> – Upgrades firmware in a specified RF Domain. Specify the RF Domain name. • all – Upgrades firmware on all RF Domains
[all|br650|br6511| br71xx]	After specifying the RF Domain, select the AP type. • all – Upgrades firmware on all APs • 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 71XX Access Point – Upgrades firmware on all Brocade Mobility 71XX Access Points
upgrade <TIME>	Schedules AP 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 wireless controller must be manually restarted) • no-reboot – Optional. Disables automatic reboot after a successful upgrade (the wireless controller 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

Example

```
rfs7000-37FABE>ap-upgrade all
-------------------------------------------------------------------------------
---
         CONTROLLER           STATUS                    MESSAGE
-------------------------------------------------------------------------------
---
  00-15-70-37-FA-BE         Fail         Could not find any matching APs
-------------------------------------------------------------------------------
---
rfs7000-37FABE>

rfs7000-37FABE>ap-upgrade default/ap no-reboot
```

```
-------------------------------------------------------------------------------
---
         CONTROLLER              STATUS                    MESSAGE
-------------------------------------------------------------------------------
---
  00-15-70-37-FA-BE          Success          Queued 0 APs to upgrade
-------------------------------------------------------------------------------
---
rfs7000-37FABE>
```

captive-portal-page-upload

User Exec Commands

Uploads captive portal advanced pages

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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]
          {no-via-rf-domain} {(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 specified AP • <MAC/HOSTNAME> – Specify AP's MAC address or hostname.
all	Uploads 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]
{no-via-rf-domain} {(upload-time <TIME>)}
```

captive-portal-page-upload <CAPTIVE-PORTAL-NAME>	Uploads advanced pages of the captive portal 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 access points within a specified RF Domain or all RF Domains • <DOMAIN- NAME> – Uploads APs within a specified RF Domain. Specify the RF Domain name. • all – Uploads APs across all RF Domains
no-via-rf-domain	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 scheduled upload to a specified AP. Specify 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) • <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

```
rfs7000-37FABE>captive-portal-page-upload test 00-04-96-4A-A7-08 upload-time
07/15/2012-12:30
--------------------------------------------------------------------------------
---
         CONTROLLER           STATUS                    MESSAGE
--------------------------------------------------------------------------------
---
  00-15-70-37-FA-BE         Fail         Failed to initiate page upload
--------------------------------------------------------------------------------
---
rfs7000-37FABE>

rfs7000-37FABE>captive-portal-page-upload cancel-upload 00-04-96-4A-A7-08
```

```
-------------------------------------------------------------------------------
---
         CONTROLLER             STATUS                    MESSAGE
-------------------------------------------------------------------------------
---
  00-15-70-37-FA-BE         Success         Cancelled upgrade of 1 APs
-------------------------------------------------------------------------------
---
rfs7000-37FABE>
```

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

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

Parameters

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

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

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 varies depending on the mode where the clear command is executed.

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

NOTE
Refer to the interface details below when using `clear`
- ge <index> – Brocade Mobility RFS4000 supports 5GEs and 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|crypto|event-history|ip|lldp|rtls|spanning-tree|vrrp]

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

clear [cdp|lldp] neighbors {on <DEVICE-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 ip [dhcp|ospf]
clear ip dhcp bindings [<IP>|all] {on <DEVICE-NAME>}
clear ip ospf process {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>|ge <1-4>|me1|
          port-channel <1-2>|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 an AP or wireless controller. 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 AP or wireless controller • <DEVICE-NAME> – Specify the name of the AP or wireless controller.

`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 AP or wireless controller • <DEVICE-NAME> – Specify the name of the AP or wireless controller.

`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 AP or wireless controller • <DEVICE-NAME> – Specify the name of the AP or wireless controller.

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

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

`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 bindings 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 AP or wireless controller • <DEVICE-NAME> – Specify the name of the AP or wireless controller

`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 AP or wireless controller 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 or wireless controller

`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 AP or wireless controller
<DEVICE-OR-DOMAIN-NAME>	This keyword is common to all of the above. • <DEVICE-OR-DOMAIN-NAME> – Optional. Clears Aeroscout or Ekahau RTLS statistics on a specified AP, wireless controller, 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 protocol on a specified AP or wireless controller • <DEVICE-NAME> – Specify the name of the AP or wireless controller.

`clear spanning-tree detected-protocols {interface [<INTERFACE>|ge <1-4>|me1|port-channel <1-2>|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>| ge <1-4>|me1| port-channel <1-2>| pppoe1|vlan <1-4094>| wwan1]	Optional. Clears spanning tree protocols on different interfaces • <INTERFACE> – Clears detected spanning tree protocol on a specified interface. Specify the interface name. • ge <1-4> – Clears detected spanning tree protocol for the selected Gigabit Ethernet interface. Select the GigabitEthernet interface index from 1 - 4. • me1 – Clears FastEthernet interface status (up1 - Clears the uplink interface) • port-channel <1-2> – Clears detected spanning tree protocol for the selected port channel interface. Select the port channel index from 1 - 2. • pppoe1 – Clears detected spanning tree protocol for *Point-to-Point Protocol over Ethernet* (PPPoE) interface. • vlan <1-4094> – Clears detected spanning tree protocol for the selected VLAN interface. Select a *Switch Virtual Interface* (SVI) VLAN ID from 1- 4094. • wwan1 – Clears detected spanning tree protocol for wireless WAN interface.
on <DEVICE-NAME>	Optional. Clears spanning tree protocol entries on a selected AP or wireless controller • <DEVICE-NAME> – Specify the name of the AP or wireless controller.

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

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

Example

```
rfs7000-37FABE>clear event-history

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

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

rfs7000-37FABE>clear spanning-tree detected-protocols interface ge 1

rfs7000-37FABE>clear lldp neighbors


rfs7000-37FABE>show cdp neighbors
-------------------------------------------------------------------------------
---
   Device ID     Neighbor IP       Platform     Local Intrfce Port ID   Duplex
-------------------------------------------------------------------------------
---
 rfs4000-880DA7 172.16.10.8   RFS-4011-11110-US ge1           ge1     full
 rfs6000-380649 192.168.0.1   Brocade Mobility RFS6000          ge1
ge1     full
 br7131-139B34  172.16.10.22  BR7131N           ge1           ge1     full
 br7131-4AA708  169.254.167.8 BR7131N-WW        ge1           ge1     full
-------------------------------------------------------------------------------
---
rfs7000-37FABE>

rfs7000-37FABE>clear cdp neighbors

rfs7000-37FABE>show cdp neighbors
-------------------------------------------------------------------------------
---
  Device ID    Neighbor IP     Platform   Local Intrfce    Port ID     Duplex
-------------------------------------------------------------------------------
---
-------------------------------------------------------------------------------
---
rfs7000-37FABE>
```

clock

User Exec Commands

Sets a device's system clock

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 or wireless controller.

Example

```
rfs7000-37FABE>clock set 14:43:20 07 May 2012
rfs7000-37FABE>show clock
2012-05-07 14:43:23 UTC
rfs7000-37FABE>
```

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:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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, as a member, to an existing cluster of wireless 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 the 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 01.42.14.79:
LSP 01.42.14.79 at level 1, hostname "rfs7000-37FABE", 1 adjacencies, seqnum
5069
LSP 01.44.54.C0 at level 1, hostname "br650-4454C0", 1 adjacencies, seqnum
5265

rfs7000-37FABE>connect mint-id 01.44.54.C0

Entering character mode
Escape character is '^]'.

br650 release 5.4.0.0-033B
br650-4454C0 login:


rfs7000-37FABE>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
65562
rfs7000-37FABE>

rfs7000-37FABE>connect rfs7000-37FABE

Entering character mode
Escape character is '^]'.

Brocade Mobility RFS7000 release 5.4.0.0-015D
rfs7000-37FABE login:
```

create-cluster

User Exec Commands

Creates a new cluster on a specified device

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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
ip <IP>	Specifies the device's IP address used for cluster creation • <IP> – Specify the device's IP address in 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>
```

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 wireless controller, as a member, to an existing cluster of wireless controllers

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
crypto [key|pki]

crypto key [export|generate|import|zeroise]

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 zeroise rsa <RSA-KEYPAIR-NAME> {force {on <DEVICE-NAME>}|on
<DEVICE-   NAME>}

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

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 [url <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> [url <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 zeroise 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 (AP/wireless controller) 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 or wireless controller.

```
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 or wireless controller.

`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 or wireless controller.

`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 or wireless controller.
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 or wireless controller.

`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 or wireless controller.

`crypto key zeroise <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.
zeroise rsa <RSA-KEYPAIR-NAME>	Deletes a specified RSA Keypair • <RSA-KEYPAIR-NAME> – Specify the RSA Keypair name. 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 (AP/wireless controller) 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 or wireless controller.

`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 The CA certificate is imported from the specified location.
background {on <DEVICE-NAME>}	Optional. Performs authentication in the background. Optionally specify a device (AP/wireless controller) on which to perform authentication.
on <DEVICE-NAME>	Optional. Performs authentication on a specified device • <DEVICE-NAME> – Specify the name of the AP or wireless controller.

`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 *Certificate Signing Request* (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 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 or wireless controller.
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>
[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 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)

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 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 or wireless controller.
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 or wireless controller.
on <DEVICE-NAME>	Optional. Performs export operation on a specified device • <DEVICE-NAME> – Specify the name of the AP or wireless controller.
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 or wireless controller.

```
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>	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.
on <DEVICE-NAME>	Exports the CSR on a specified device • <DEVICE-NAME> – Specify the name of the AP or wireless controller.

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

`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 or wireless controller.

on <DEVICE-NAME>	Optional. Performs import operation on a specified device • <DEVICE-NAME> – Specify the name of the AP or wireless controller.
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 or wireless controller.

```
crypto pki zeroise 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.
zeroise <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 or wireless controller.
on <DEVICE-NAME>	Optional. Deletes the trustpoint on a specified device • <DEVICE-NAME> – Specify the name of the AP or wireless controller.

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>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

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
enable
```

Parameters

None

Example

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

join-cluster

User Exec Commands

Adds a wireless controller, as a member, to an existing cluster of wireless controllers. Use this command to add a new wireless controller to an existing cluster. Before adding the wireless controller, assign a static IP address.

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 new wireless controller 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 wireless controller to an existing cluster:

- Configure a static IP address on the wireless controller.
- Provide username and password for superuser, network admin, system admin, or operator accounts.

Once a wireless controller is added to the cluster, a manual "write memory" command must be executed. Without this command, the configuration will not persist across reboots.

Example

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

rfs7000-37FABE#
```

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 a *Layer 2 Tunnel Protocol Version 3* (L2TPV3) tunnel

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 tunnel
<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 or wireless controller.

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

l2tpv3 tunnel	Establishes or brings downs L2TPV3 tunnel
<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 or wireless controller.

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

l2tpv3 tunnel	Establishes or brings down 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 or wireless controller.

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 24, L2TPV3-Policy*.

logging

User Exec Commands

Modifies message logging settings

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

```
rfs7000-37FABE>logging monitor warnings
rfs7000-37FABE>show logging
Logging module: enabled
    Aggregation time: disabled
    Console logging: level warnings
    Monitor logging: level warnings
    Buffered logging: level warnings
    Syslog logging: level warnings
        Facility: local7

Log Buffer (18611 bytes):

Mar 14 14:52:22 2012: %AUTHPRIV-4-WARNING: pluto[1304]: inserting event
EVENT_REINIT_SECRET, timeout in 3600 seconds
Mar 14 14:51:29 2012: %CERTMGR-4-CERT_EXPIRY: server certificate for
trustpoint mint_security_trustpoint Certificate has expired. Valid until: Tue
Apr 26 15:00:41 2011 UTC, current time: Wed Mar 14 14:51:29 2012 UTC
Mar 14 14:51:29 2012: %CERTMGR-4-CERT_EXPIRY: ca certificate for trustpoint
mint_security_trustpoint Certificate has expired. Valid until: Tue Apr 26
15:00:39 2011 UTC, current time: Wed Mar 14 14:51:29 2012 UTC
--More--
```

Related Commands:

no	Resets terminal lines logging levels

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
exit
```

Parameters

None

Example

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

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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. 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
```

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
no [adoption|captive-portal|crypto|debug|logging|page|service|terminal|
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 [br300|locator]
no service br300 locator <MAC>
no service locator {on <DEVICE-NAME>}
```

```
no terminal [length|width]

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 adopted by a device • <DEVICE-OR-DOMAIN-NAME> – Optional. Specify the name of the AP, wireless controller, or RF 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 captive portal clients • <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, 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 will fail 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 or wireless controller.

```
no logging monitor
```

no logging monitor	Resets terminal lines message logging levels

```
no page
```

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

	`no service br300 locator <MAC>`
no service	Disables LEDs on Brocade Mobility 300 Access Points or a specified device in the WLAN. It also resets the CLI table expand and MiNT protocol configurations.
no br300 locator <MAC>	Disables LEDs on Brocade Mobility 300 Access Points • <MAC> – Specify the Brocade Mobility 300 Access Point's MAC address.

	`no service locator {on <DEVICE-NAME>}`
no service	Disables LEDs on Brocade Mobility 300 Access Points or 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 • on <DEVICE-NAME> – Optional. Specify the name of the AP or wireless controller.

	`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 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, 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, 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 the wireless 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
wireless-client	Manages wireless clients

page

User Exec Commands

Toggles wireless 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
page
```

Parameters

None

Example

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

Related Commands:

no	Disables wireless controller 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

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

Parameters

```
ping <IP/HOSTNAME> {count <1-10000>|dont-fragment|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	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.
size <1-64000>	Optional. Sets the size of ping payload 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

```
rfs7000-37FABE>telnet 172.16.10.4

Entering character mode
Escape character is '^]'.


Brocade Mobility RFS6000 release 5.4.0.0-032R
rfs6000-380649 login: admin
Password:
rfs6000-380649>
```

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 a 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 of the terminal window or the number of lines displayed within 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 sec - 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>
```

2

Chapter

Privileged Exec Mode Commands

3

In this chapter

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:

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

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.

```
rfs7000-37FABE#?
Privileged command commands:
  ap-upgrade                  AP firmware upgrade
  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.
  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
  format                      Format file system
  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
  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
  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
  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

rfs7000-37FABE#
```

Privileged Exec Mode Commands

Table 2 summarizes PRIV EXEC Mode commands.

TABLE 2 Privileged Exec Commands

Command	Description	Reference
ap-upgrade	Enables an automatic firmware upgrade on an adopted AP	*page 3-58*
archive	Manages file archive operations	*page 3-63*
boot	Specifies the image used after reboot	*page 3-64*
captive-portal-page-upload	Uploads captive portal advanced pages	*page 3-65*
cd	Changes the current directory	*page 3-67*
change-passwd	Changes the password of a logged user	*page 3-67*
clear	Clears parameters, cache entries, table entries, and other similar entries	*page 3-68*
clock	Configures the system clock	*page 3-72*

TABLE 2 Privileged Exec Commands

Command	Description	Reference
cluster	Initiates a cluster context	*page 3-73*
configure	Enters the configuration mode	*page 3-74*
connect	Begins a console connection to a remote device	*page 3-74*
copy	Copies a file from any location to the wireless controller	*page 3-75*
create-cluster	Creates a new cluster on a specified device	*page 3-76*
crypto	Enables encryption	*page 3-77*
delete	Deletes a specified file from the system	*page 3-86*
diff	Displays the differences between two files	*page 3-87*
dir	Displays the list of files on a file system	*page 3-88*
disable	Disables the privileged mode command set	*page 3-89*
edit	Edits a text file	*page 3-89*
enable	Turns on (enables) the privileged mode commands set	*page 3-90*
erase	Erases a file system	*page 3-91*
exit	Ends the current CLI session and closes the session window	*page 3-92*
format	Formats the file system	*page 3-92*
halt	Halts a device or a wireless controller.	*page 3-93*
join-cluster	Adds a wireless controller, as cluster member, to an existing cluster of wireless controllers	*page 3-93*
l2tpv3	Establishes or brings down *Layer 2 Tunneling Protocol Version* 3 (L2TPV3) tunnel	*page 3-94*
logging	Modifies message logging parameters	*page 3-95*
mint	Configures MiNT protocols	*page 3-96*
mkdir	Creates a new directory in the file system	*page 3-98*
more	Displays the contents of a file	*page 3-99*
no	Reverts a command or sets values to their default settings	*page 3-100*
page	Toggles wireless controller paging	*page 3-103*
ping	Sends ICMP echo messages to a user-specified location	*page 3-104*
pwd	Displays the current directory	*page 3-105*
re-elect	Re-elects tunnel wireless controller	*page 3-105*
reload	Halts the wireless controller and performs a warm reboot	*page 3-106*
remote-debug	Troubleshoots remote systems	*page 3-107*
rename	Renames a file in the existing file system	*page 3-109*
rmdir	Deletes an existing file from the file system	*page 3-110*
self	Displays the configuration context of the device	*page 3-110*
ssh	Connects to another device using a secure shell	*page 3-111*
telnet	Opens a Telnet session	*page 3-112*
terminal	Sets the length/number of lines displayed within the terminal window	*page 3-112*
time-it	Verifies the time taken by a particular command between request and response	*page 3-113*

TABLE 2 Privileged Exec Commands

Command	Description	Reference
traceroute	Traces the route to a defined destination	*page 3-113*
upgrade	Upgrades the software image	*page 3-114*
upgrade-abort	Aborts an ongoing software image upgrade	*page 3-115*
watch	Repeats the specific CLI command at a periodic interval	*page 3-116*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) the changes made in the current session	*page 5-276*
help	Displays interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug (config-if) instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes information to memory or terminal	*page 5-310*

ap-upgrade

Privileged Exec Mode Commands

Enables automatic firmware upgrade on an adopted AP or a set of APs. APs of the same type can be upgraded together. Once APs have been upgraded, they can be forced to reboot.

The AP upgrade command also upgrades APs in a specified RF Domain.

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
ap-upgrade [<MAC/HOSTNAME>|all|br650|br6511|br71xx|
           cancel-upgrade|load-image|rf-domain]

ap-upgrade [<MAC/HOSTNAME>] {no-reboot|reboot-time <TIME>|
           upgrade-time <TIME> {no-reboot|reboot-time <TIME>}}

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

ap-upgrade [br650|br6511|br71xx] all
   {no-reboot|reboot-time <TIME>|upgrade-time <TIME> {no-reboot|reboot-time
<TIME>}}
           {(staggered-reboot)}]

ap-upgrade cancel-upgrade [<MAC/HOSTNAME>|all|br650|br6511||
           br71xx|on]
ap-upgrade cancel-upgrade [<MAC/HOSTNAME>|all]
ap-upgrade cancel-upgrade [br650|br6511|br71xx] all
ap-upgrade cancel-upgrade on rf-domain [<RF-DOMAIN-NAME>|all]
```

```
ap-upgrade load-image [br650|br6511|br71xx]
          <IMAGE-URL>

ap-upgrade rf-domain [<RF-DOMAIN-NAME>|all] [all|br650|br6511|
          br71xx] {no-reboot|no-via-rf-domain|reboot-time <TIME>|
          staggered-reboot|upgrade-time <TIME>}

ap-upgrade rf-domain [<RF-DOMAIN-NAME>|all] [all|br650|br6511|
          br71xx] {no-reboot {staggered-reboot}|
          reboot-time <TIME> {staggered-reboot}}

ap-upgrade rf-domain [<RF-DOMAIN-NAME>|all] [all|br650|br6511|
          br71xx] {no-via-rf-domain {no-reboot|reboot-time <TIME>|
          upgrade-time <TIME> {no-reboot|reboot-time <TIME>}}}
{(staggered-reboot)}

ap-upgrade rf-domain [<RF-DOMAIN-NAME>|all] [all|br650|br6511|
          br71xx] {upgrade-time <TIME> {no-reboot|reboot-time <TIME>}}
          {(staggered-reboot)}
```

Parameters

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

<MAC/HOSTNAME>	Upgrades firmware on a specified AP or all APs adopted by the wireless controller • <MAC/HOSTNAME> – Specify the AP's MAC address or hostname.
no-reboot	Optional. Disables automatic reboot after a successful upgrade (the wireless controller 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 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 wireless controller 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.

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

all	Upgrades firmware on all APs adopted by the wireless controller
no-reboot	Optional. Disables automatic reboot after a successful upgrade (the wireless controller 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 firmware upgrade on all adopted APs • <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 wireless controller 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
	`ap-upgrade [br650|br6511|br71xx] all` *`{no-reboot|reboot-time <TIME>|upgrade-time <TIME> {no-reboot|reboot-time <TIME>}} {(staggered-reboot)}`*
[br650|br6511 |br71xx] all	Upgrades firmware on all adopted APs • 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 71XX Access Point all – Upgrades firmware on all Brocade Mobility 71XX Access Points After selecting the AP type, you can schedule an automatic upgrade and/or an automatic reboot.
no-reboot	Optional. Disables automatic reboot after a successful upgrade (the wireless controller 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 firmware upgrade on an AP adopted by the wireless controller • <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 wireless controller 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
	`ap-upgrade cancel-upgrade [<MAC/HOSTNAME>|all]`
cancel-upgrade [<MAC/HOSTNAME>| all]	Cancels a scheduled firmware upgrade on a specified AP or all APs adopted by the wireless controller • <MAC/HOSTNAME> – Cancels a scheduled upgrade on a specified AP. Specify the AP's MAC address or hostname. • all – Cancels scheduled upgrade on all APs
	`ap-upgrade cancel-upgrade [br650|ap651|br71xx] all`
cancel-upgrade [br650| br6511|br71xx] all	Cancels scheduled firmware upgrade on all adopted APs • 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 71XX Access Point all – Cancels scheduled upgrade on all Brocade Mobility 71XX Access Points

`ap-upgrade cancel-upgrade on rf-domain [<DOMAIN-NAME>|all]`

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

`ap-upgrade load-image [br650|br6511|br71xx] <IMAGE-URL>`

load-image [br650| br6511|br71xx]	Loads AP firmware images on the wireless controller. Select the AP type and provide the location of the AP 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
<IMAGE-URL>	Specify the AP 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

`ap-upgrade rf-domain [<RF-DOMAIN-NAME>|all] [all|br650|br6511| br71xx] {no-reboot {staggered-reboot}|reboot-time <TIME> {staggered-reboot}}`

rf-domain [<RF-DOMAIN-NAME>| all]	Upgrades AP firmware on devices in a specified RF Domain or all RF Domains • <RF-DOMAIN-NAME> – Upgrades firmware in a specified RF Domain. Specify the RF Domain name. • all – Upgrades firmware on all RF Domains
[all|br650|br6511|br71xx]	After specifying the RF Domain, select the AP type. • all – Upgrades firmware on all APs • 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 71XX Access Point – Upgrades firmware on all Brocade Mobility 71XX Access Points
no-reboot {staggered-reboot}	Optional. Disables automatic reboot after a successful upgrade (the wireless controller must be manually restarted) • no-reboot – Optional. Disables automatic reboot after a successful upgrade (the wireless controller 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

	`ap-upgrade rf-domain [<RF-DOMAIN-NAME>|all] [all|br650|br6511|br71xx] {no-via-rf-domain {no-reboot|reboot-time <TIME>| upgrade-time <TIME> {no-reboot|reboot-time <TIME>}} {(staggered-reboot)}`
rf-domain [<RF-DOMAIN-NAME>| all]	Upgrades AP firmware on devices in a specified RF Domain or all RF Domains • <RF-DOMAIN-NAME> – Upgrades firmware in a specified RF Domain. Specify the RF Domain name. • all – Upgrades firmware on all RF Domains
[all|br650|br6511|br71xx]	After specifying the RF Domain, select the AP type. • all – Upgrades firmware on all APs • 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 71XX Access Point – Upgrades firmware on all Brocade Mobility 71XX Access Points
no-via-rf-domain	Upgrades APs from the adopted device
no-reboot {staggered-reboot}	Optional. Disables automatic reboot after a successful upgrade (the wireless controller must be manually restarted) • no-reboot – Optional. Disables automatic reboot after a successful upgrade (the wireless controller 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. The following actions can be performed after a scheduled upgrade: • no-reboot – Optional. Disables automatic reboot after a successful upgrade (the wireless controller 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

	`ap-upgrade rf-domain [<RF-DOMAIN-NAME>|all] [all|br650|br6511|br71xx] {upgrade-time <TIME> {no-reboot|reboot-time <TIME>}} {(staggered-reboot)}`
rf-domain [<RF-DOMAIN-NAME>| all]	Upgrades AP firmware on devices in a specified RF Domain or all RF Domains • <RF-DOMAIN-NAME> – Upgrades firmware in a specified RF Domain. Specify the RF Domain name. • all – Upgrades firmware on all RF Domains
[all|br650|br6511|br71xx]	After specifying the RF Domain, select the AP type. • all – Upgrades firmware on all APs • 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 71XX Access Point – Upgrades firmware on all Brocade Mobility 71XX Access Points
upgrade <TIME>	Schedules AP 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 wireless controller must be manually restarted) • no-reboot – Optional. Disables automatic reboot after a successful upgrade (the wireless controller 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

Example

```
rfs7000-37FABE#ap-upgrade all
-------------------------------------------------------------------------------
---
         CONTROLLER           STATUS                    MESSAGE
-------------------------------------------------------------------------------
---
  00-15-70-37-FA-BE         Fail         Could not find any matching APs
-------------------------------------------------------------------------------
---
rfs7000-37FABE#

rfs7000-37FABE#ap-upgrade default/ap no-reboot
-------------------------------------------------------------------------------
---
         CONTROLLER              STATUS                    MESSAGE
-------------------------------------------------------------------------------
---
  00-15-70-37-FA-BE          Success          Queued 0 APs to upgrade
-------------------------------------------------------------------------------
---
rfs7000-37FABE#
```

archive

Privileged Exec Mode Commands

Manages file archive operations

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

How to zip the folder flash:/log/?

```
rfs7000-37FABE#archive tar /create flash:/out.tar flash:/log/
log/
log/vlan-usage.log
log/dpd2.log
log/upgrade.log
log/dpd2.startup
log/cfgd.log
log/messages.log
log/startup.log
log/radius/
rfs7000-37FABE#

rfs7000-37FABE#dir flash:/
Directory of flash:/

  drwx             Fri Aug  3 13:16:52 2012   log
  drwx             Fri Jul  8 15:50:23 2011   Final
  drwx             Mon Jul 18 15:16:35 2011   cache
  drwx             Thu Jul 19 08:40:19 2012   crashinfo
  drwx             Fri Aug  3 13:14:11 2012   archived_logs
  drwx             Sat Jan  1 05:30:25 2000   hotspot
  drwx             Sat Jan  1 05:30:09 2000   floorplans
  drwx             Wed May  9 20:18:19 2012   startuplog
  -rw-   244736    Thu Aug 16 10:05:58 2012   out.tar

rfs7000-37FABE#
```

boot

Privileged Exec Mode Commands

Specifies the image used after reboot

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 a primary image after reboot • secondary – Uses a 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 or wireless controller.

Example

```
rfs7000-37FABE#boot system primary on rfs7000-37FABE
Updated system boot partition
rfs7000-37FABE#
```

captive-portal-page-upload

Privileged Exec Mode Commands

Uploads captive portal advanced pages

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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]
          {no-via-rf-domain} {(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]` *`{no-via-rf-domain} {(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 access points 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
no-via-rf-domain	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 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 specified AP. Specify 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 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

```
rfs7000-37FABE>captive-portal-page-upload test 00-04-96-4A-A7-08 upload-time
07/15/2012-12:30
------------------------------------------------------------------------------
---
          CONTROLLER            STATUS                      MESSAGE
------------------------------------------------------------------------------
---
```

```
  00-15-70-37-FA-BE         Fail         Failed to initiate page upload
-------------------------------------------------------------------------------
---
rfs7000-37FABE>

rfs7000-37FABE>captive-portal-page-upload cancel-upload 00-04-96-4A-A7-08
-------------------------------------------------------------------------------
---
         CONTROLLER             STATUS                    MESSAGE
-------------------------------------------------------------------------------
---
  00-15-70-37-FA-BE         Success         Cancelled upgrade of 1 APs
-------------------------------------------------------------------------------
---
rfs7000-37FABE>
```

cd

Privileged Exec Mode Commands

Changes the current directory

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 name.

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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. 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

NOTE
Refer to the interface details below when using clear
- ge <index> – Brocade Mobility RFS4000 supports 5GEs, Brocade Mobility RFS6000 supports 8 GEs and Brocade Mobility RFS7000 supports 4GEs
- 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|ip|lldp|
logging|rtls|
          spanning-tree|vrrp]
```

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

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

clear counters [all|bridge|interface|router|thread]
clear counters interface [<INTERFACE>|all|ge <1-4>|me1|port-channel <1-2>|
pppoe1|
          vlan <1-4094>|wwan1]

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

clear logging {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>|ge <1-4>|me1|
          port-channel <1-2>|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 an AP or wireless controller
on <DEVICE-NAME>	Optional. Clears ARP cache entries on a specified device • <DEVICE-NAME> – Specify the name of the AP or wireless controller.

`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 or wireless controller.

`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 interface [<INTERFACE>|all|ge <1-4>|me1|port-channel <1-2>|pppoe1| vlan <1-4094>|wwan1]`

counters interface [<INTERFACE>|all| ge <1-4>|me1| port-channel <1-2>| pppoe1|vlan <1-4094>| wwan1]	Clears interface counters for a specified interface • <INTERFACE> – Clears a specified interface counters. Specify the interface name. • all – Clears all interface counters • ge <1-4> – Clears GigabitEthernet interface counters. Specify the GigabitEthernet interface index from 1 - 4. • me1 – Clears FastEthernet interface counters • port-channel <1-2> – Clears port-channel interface counters. Specify the port channel interface index from 1 - 2. • 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 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 AP or wireless controller • <DEVICE-NAME> – Specify the name of the AP or wireless controller.

`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 AP or wireless controller • <DEVICE-NAME> – Specify the name of the AP or wireless controller.

`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 or wireless controller.

`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 AP or wireless controller • <DEVICE-NAME> – Specify the name of the AP or wireless controller.

`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 *Open Shortest Path First* (OSPF) process on a specified AP or wireless controller 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 or wireless controller.

`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 AP or wireless controller
<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 AP, wireless controller, 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 or wireless controller.

`clear spanning-tree detected-protocols {interface [<INTERFACE>|ge <1-4>|me1| port-channel <1-2>|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>| ge <1-4>|me1| port-channel <1-2>| pppoe1|vlan <1-4094>| wwan1]	Optional. Clears spanning tree protocols on different interfaces • <INTERFACE> – Clears detected spanning tree protocol on a specified interface. Specify the interface name. • ge <1-4> – Clears detected spanning tree protocol for the selected GigabitEthernet interface. Select the GigabitEthernet interface index from 1 - 4. • me1 – Clears FastEthernet interface status (up1 - Clears the uplink interface) • port-channel <1-2> – Clears detected spanning tree protocol for the selected port channel interface. Select the port channel index from 1 - 2. • pppoe1 – Clears detected spanning tree protocol for *Point-to-Point Protocol over Ethernet* (PPPoE) interface. • vlan <1-4094> – Clears detected spanning tree protocol for the selected VLAN interface. Select a SVI VLAN ID from 1- 4094. • wwan1 – Clears detected spanning tree protocol for wireless WAN interface.
on <DEVICE-NAME>	Optional. Clears spanning tree protocol entries on a selected AP or wireless controller • <DEVICE-NAME> – Specify the name of the AP or wireless controller.

`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 AP or wireless controller • <DEVICE-NAME> – Specify the name of the AP or wireless controller.
stats {on <DEVICE-NAME>}	Clears VRRP related statistics • on <DEVICE-NAME> – Optional. Clears VRRP related statistics on a selected AP or wireless controller • <DEVICE-NAME> – Specify the name of the AP or wireless controller.

Example

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

rfs7000-37FABE>clear event-history
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#

rfs4000-880DA7#clear spanning-tree detected-protocols interface ge 1
rfs4000-880DA7#

rfs4000-880DA7#clear lldp neighbors
rfs4000-880DA7#
```

clock

Privileged Exec Mode Commands

Sets a device's system clock

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 or wireless controller.

Example

```
rfs7000-37FABE#clock set 16:01:45 20 Mar 2012 on rfs7000-37FABE
rfs7000-37FABE#

rfs7000-37FABE#show clock
2012-03-20 16:01:53 UTC
rfs7000-37FABE#
```

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:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 wireless 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

```
rfs7000-37FABE#connect mint-id 01.4A.A7.08

Entering character mode
Escape character is '^]'.

BR7131 release 5.4.0.0-015D
BR7131N login: admin
Password:
BR7131N>

rfs7000-37FABE#show mint lsp-db on rfs7000-37FABE
3 LSPs in LSP-db of 70.37.FA.BE:
LSP 01.4A.A7.08 at level 1, hostname "BR7131N", 2 adjacencies, seqnum 284
LSP 70.37.FA.BE at level 1, hostname "rfs7000-37FABE", 1 adjacencies, seqnum
83325
LSP 70.38.06.49 at level 1, hostname "rfs6000-380649", 1 adjacencies, seqnum
9275
rfs7000-37FABE#

rfs7000-37FABE#connect mint-id 70.38.06.49

Entering character mode
Escape character is '^]'.Brocade Mobility RFS6000 release 5.2.3.0-032R
rfs6000-380649 login: admin
Password:
rfs6000-380649>
```

copy

Privileged Exec Mode Commands

Copies a file (config,log,txt...etc) from any location to the wireless controller 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 cluster on a specified device

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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.

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>
```

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, 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 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
crypto [key|pki]

crypto key [export|generate|import|zeroise]

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 zeroise rsa <RSA-KEYPAIR-NAME> {force {on <DEVICE-NAME>}|on
<DEVICE-   NAME>}

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

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 [url <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> [url <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 zeroise 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 (AP/wireless controller) to export to.
on <DEVICE-NAME>	Optional. Performs an export operation to a specific device. • <DEVICE-NAME> – Specify the name of the AP or wireless controller.

`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 or wireless controller.

`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 or wireless controller.

`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 or wireless controller.
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 or wireless controller.

`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 or wireless controller.

`crypto key zeroise <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.
zeroise rsa <RSA-KEYPAIR-NAME>	Deletes a specified RSA Keypair • <RSA-KEYPAIR-NAME> – Specify the RSA Keypair name. 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 (AP/wireless controller) 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 or wireless controller.

`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 The CA certificate is imported from the specified location.
background {on <DEVICE-NAME>}	Optional. Performs authentication in the background. Optionally specify a device (AP/wireless controller) on which to perform authentication.
on <DEVICE-NAME>	Optional. Performs authentication on a specified device • <DEVICE-NAME> – Specify the name of the AP or wireless controller.

```
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 *Certificate Signing Request* (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 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 to a specified device • <DEVICE-NAME> – Specify the name of the AP or wireless controller.
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> [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 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)
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 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 to a specific device • <DEVICE-NAME> – Specify the name of the AP or wireless controller.
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 to a specified device • <DEVICE-NAME> – Specify the name of the AP or wireless controller.
on <DEVICE-NAME>	Optional. Performs an export operation to a specified device • <DEVICE-NAME> – Specify the name of the AP or wireless controller.
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 an export operation in the background • on <DEVICE-NAME> – Optional. Performs an export operation to a specified device • <DEVICE-NAME> – Specify the name of the AP or wireless controller.

```
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>	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.
on <DEVICE-NAME>	Exports the CSR on a specified device • <DEVICE-NAME> – Specify the name of the AP or wireless controller.

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

```
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 or wireless controller.
on <DEVICE-NAME>	Optional. Performs import operation on a specified device • <DEVICE-NAME> – Specify the name of the AP or wireless controller.
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 or wireless controller.

```
crypto pki zeroise 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.
zeroise <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 or wireless controller.
on <DEVICE-NAME>	Optional. Deletes the trustpoint on a specified device • <DEVICE-NAME> – Specify the name of the AP or wireless controller.

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>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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

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

Parameters

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

/force	Forces deletion without a prompt
/recursive	Performs a recursive delete
<FILE>	Specifies the filenames to delete

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#
```

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

```
rfs7000-37FABE#diff startup-config running-config
--- startup-config
+++ running-config
@@ -1,3 +1,4 @@
+!### show running-config
 !
 ! Configuration of Brocade Mobility RFS7000 version 5.4.0.0-015D
 !
@@ -327,44 +328,38 @@
  logging buffered warnings
 !
 br71xx 00-04-96-4A-A7-08
- radio-count 2
  use profile default-br71xx
```

```
  use rf-domain default
- hostname br71xx-4AA708
- license AP VIRTUAL_CONTROLLER_DEFAULT_AP_LICENSE
- no staging-config-learnt
- model-number Brocade Mobility 7131 Access PointN-WW
+ hostname Brocade Mobility 7131 Access PointN
+ ip default-gateway 172.16.10.7
+ interface vlan1
+  ip address 172.16.10.23/24
+ controller host 172.16.10.7
--More--
```

dir

Privileged Exec Mode Commands

Lists files on a device's file system

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

```
rfs7000-37FABE#dir
Directory of flash:/.

  drwx             Wed Mar 21 04:08:22 2012   log
  drwx             Fri Jul  8 10:20:23 2011   test
  drwx             Mon Jul 18 09:46:35 2011   cache
  drwx             Tue Mar 20 10:11:09 2012   crashinfo
  drwx             Sat Jan  1 00:00:25 2000   hotspot
  drwx             Sat Jan  1 00:00:09 2000   floorplans
  drwx             Mon Mar 19 13:57:43 2012   startuplog
  -rw-   373760    Thu Mar 15 12:15:07 2012   out.tar

rfs7000-37FABE#

rfs7000-37FABE#dir all-filesystems
Directory of flash:/

  drwx             Wed Mar 21 04:08:22 2012   log
```

```
  drwx             Fri Jul  8 10:20:23 2011   test
  drwx             Mon Jul 18 09:46:35 2011   cache
  drwx             Tue Mar 20 10:11:09 2012   crashinfo
  drwx             Sat Jan  1 00:00:25 2000   hotspot
  drwx             Sat Jan  1 00:00:09 2000   floorplans
  drwx             Mon Mar 19 13:57:43 2012   startuplog
  -rw-   373760    Thu Mar 15 12:15:07 2012   out.tar

Directory of nvram:/

  -rw-   3460      Fri Dec 11 14:42:44 2009   startup-config.save
  -rw-   1638      Tue Jan  5 14:27:17 2010   startup-config-unused
  -rw-   3393      Mon Dec 14 13:55:51 2009   startup-config.save.1
  -rw-   9392      Fri Dec  2 10:33:40 2011   startup-config.save.2
  -rw-   8192      Fri Dec  2 10:39:58 2011   startup-config.save.3
  -rw-   9395      Fri Dec  2 10:39:58 2011   startup-config.save.4
  -rw-   185       Mon Mar 19 13:57:31 2012   licenses
  -rw-   9728      Tue Mar 20 12:52:56 2012   startup-config

Directory of system:/

--More--
rfs7000-37FABE#
```

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
edit <FILE>
```

Parameters

```
edit <FILE>
```

<FILE>	Specify the name of the file to modify.

Example

```
rfs7000-37FABE#edit startup-config
   GNU nano 1.2.4               File: startup-config

!
! Configuration of Brocade Mobility RFS7000 version 5.4.0.0-015D

!
!
version 2.1
!
!
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
$
 permit ip any any rule-precedence 100 rule-description "permit all IP
traffic"
!
ip access-list test
!
mac access-list PERMIT-ARP-AND-IPv4
 permit any any type ip rule-precedence 10 rule-description "permit all IPv4
tr$
                              [ Read 353 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
enable
```

Parameters

None

Example

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

erase

Privileged Exec Mode Commands

Erases a device's 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
erase [cf:|flash:|nvram:|startup-config|usb1:|usb2:]
```

Parameters

```
erase [cf:|flash:|nvram:|startup-config|usb1:|usb2:]
```

cf:	Erases everything in the wireless controller cf: file
flash:	Erases everything in the wireless controller flash: file
nvram:	Erases everything in the wireless controller nvram: file
startup-config	Erases the wireless controller's startup configuration file. The startup configuration file is used to configure the device when it reboots.
usb1:	Erases everything in the wireless controller usb1: file
usb2:	Erases everything in the wireless controller usb2: file

Example

```
rfs7000-37FABE#erase startup-config
Erase startup-config? (y/n): n
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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
exit
```

Parameters

None

Example

```
rfs7000-37FABE#exit
```

format

Privileged Exec Mode Commands

Formats the device's compact flash file system

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
format cf:
```

Parameters

```
format cf:
```

cf:	Formats the compact flash file system

Example

```
rfs7000-37FABE#format cf:

Warning: This will destroy the contents of compact flash.
Do you want to continue [y/n]? n

rfs7000-37FABE#
```

halt

Privileged Exec Mode Commands

Stops (halts) a device or a wireless controller. 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
halt {on <DEVICE-NAME>}
```

Parameters

```
halt {on <DEVICE-NAME>}
```

halt {on <DEVICE-NAME>}	Halts a device or a wireless controller • on <DEVICE-NAME> – Optional. Enter the name of the AP or wireless controller.

Example

```
rfs7000-37FABE#halt on rfs7000-37FABE
rfs7000-37FABE#
```

join-cluster

Privileged Exec Mode Commands

Adds a wireless controller, as cluster member, to an existing cluster of wireless controllers. Use this command to add a new wireless controller to an existing cluster. Before a wireless controller can be added to a cluster, a static address must be assigned to it.

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

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

Parameters

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

join-cluster	Adds a new wireless controller 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]	Configures the routing level • 1 – Configures level 1 routing • 2 – Configures level 2 routing
mode [active|standby]	Configures the cluster mode • active – Configures cluster mode as active • standby – Configures cluster mode as standby

Usage Guidelines:

To add a wireless controller to an existing cluster:

- Configure a static IP address on the wireless controller.
- Provide username and password for superuser, network admin, system admin, or operator accounts.

Once a wireless controller is added to the cluster, a manual "write memory" command must be executed. Without this command, the configuration will not persist across reboots.

Example

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

rfs7000-37FABE#
```

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 a L2TPV3 tunnel

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 a 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 or wireless controller.

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

l2tpv3 tunnel <TUNNEL-NAME>	Establishes or brings down a 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 or wireless controller.

`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 or wireless controller.

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 24,* .

logging

Privileged Exec Mode Commands

Modifies message logging settings

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
mint [ping|security|traceroute]

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

mint security [approve-request [<MAC>|all]|create-security-trustpoint]

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 security [approve-request [<MAC>|all]|create-security-trustpoint]`

security	Invokes MiNT security commands
approve request [<MAC>|all]	Approves requests to join MiNT security domain • <MAC> – Approves request from a specific device. Specify the device's MAC address. • all – Approves all pending requests.
create-security-trustpoint	Creates a new trustpoint to use with MiNT

`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
```

mkdir

Privileged Exec Mode Commands

Creates a new directory in the file system

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
mkdir <DIR>
```

Parameters

```
mkdir <DIR>
```

<DIR>	Specify a directory name. A directory, specified by the <DIR> parameter, is created within the file system.

Example

```
rfs7000-37FABE#dir
Directory of flash:/.

  drwx             Wed Mar 21 14:19:34 2012   log
  drwx             Fri Jul  8 10:20:23 2011   test
  drwx             Mon Jul 18 09:46:35 2011   cache
  drwx             Tue Mar 20 10:11:09 2012   crashinfo
  drwx             Sat Jan  1 00:00:25 2000   hotspot
  drwx             Sat Jan  1 00:00:09 2000   floorplans
  drwx             Mon Mar 19 13:57:43 2012   startuplog
  -rw-   373760    Thu Mar 15 12:15:07 2012   out.tar

rfs7000-37FABE#

rfs7000-37FABE#mkdir testdir
rfs7000-37FABE#
```

```
rfs7000-37FABE#dir
Directory of flash:/.

  drwx             Wed Mar 21 14:19:34 2012   log
  drwx             Fri Jul  8 10:20:23 2011   test
  drwx             Mon Jul 18 09:46:35 2011   cache
  drwx             Tue Mar 20 10:11:09 2012   crashinfo
  drwx             Wed Mar 21 14:24:00 2012   testdir
  drwx             Sat Jan  1 00:00:25 2000   hotspot
  drwx             Sat Jan  1 00:00:09 2000   floorplans
  drwx             Mon Mar 19 13:57:43 2012   startuplog
  -rw-   373760    Thu Mar 15 12:15:07 2012   out.tar

rfs7000-37FABE#
```

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
more <FILE>
```

Parameters

```
more <FILE>
```

<FILE>	Specify the file name and location.

Example

```
rfs7000-37FABE#more flash:/log/messages.log
Mar 19 13:57:43 2012: %AUTHPRIV-4-WARNING: ipsec_starter[1308]: Starting
strongSwan 4.5.0 IPsec [starter]...
Mar 19 13:57:43 2012: %AUTHPRIV-4-WARNING: ipsec_starter[1308]: no default
route - cannot cope with %defaultroute!!!
Mar 19 13:57:43 2012: %AUTHPRIV-4-WARNING: ipsec_starter[1318]: pluto (1319)
started after 500 ms
Mar 19 13:57:44 2012: %AUTHPRIV-4-WARNING: pluto[1319]: inserting event
EVENT_REINIT_SECRET, timeout in 3600 seconds
Mar 19 13:57:44 2012: %AUTHPRIV-4-WARNING: pluto[1319]:   including
NAT-Traversal patch (Version 0.6c)
Mar 19 13:57:44 2012: %AUTHPRIV-4-WARNING: pluto[1319]: Changing to directory
'/var/etc/ipsec.d/crls'
Mar 19 13:57:44 2012: %AUTHPRIV-4-WARNING: pluto[1319]: inserting event
EVENT_LOG_DAILY, timeout in 36136 seconds
```

```
Mar 19 13:57:44 2012: %AUTHPRIV-4-WARNING: pluto[1319]: listening for IKE
messages
Mar 19 13:57:44 2012: %AUTHPRIV-4-WARNING: pluto[1319]: adding interface
vlan1/vlan1 172.16.10.1:500
Mar 19 13:57:44 2012: %AUTHPRIV-4-WARNING: pluto[1319]: adding interface
vlan1/vlan1 172.16.10.1:4500
Mar 19 13:57:44 2012: %AUTHPRIV-4-WARNING: pluto[1319]: adding interface
pkt0/pkt0 127.0.1.1:500
Mar 19 13:57:44 2012: %AUTHPRIV-4-WARNING: pluto[1319]: adding interface
pkt0/pk
--More--
rfs7000-37FABE#
```

no

Privileged Exec Mode Commands

Use the no command to revert a command or set parameters to their default. This command is useful to turn off an enabled feature or set defaults for a parameter.

The no commands have their own set of parameters that can be reset.

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
no [adoption|captive-portal|crypto|debug|logging|page|service|terminal|
upgrade|
          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 [br300|locator|mint]
no service br300 locator <MAC>
no service locator {on <DEVICE-NAME>}
no service mint silence

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 • <DEVICE-OR-DOMAIN-NAME> – Optional. Enter the name of the AP, wireless controller, or RF Domain.

`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 captive portal clients or a specified client on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, 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 will fail 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 or wireless controller.

`no logging monitor`

no logging monitor	Resets terminal lines message logging levels

`no page`

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

	`no service br300 locator <MAC>`
no service	Disables LEDs on Brocade Mobility 300 Access Points or a specified device in the WLAN. It also resets the CLI table and MiNT protocol configurations.
br300 locator <MAC>	Disables LEDs on Brocade Mobility 300 Access Points • <MAC> – Specify the Brocade Mobility 300 Access Point's MAC address.

	`no service locator {on <DEVICE-NAME>}`
no service	Disables LEDs on Brocade Mobility 300 Access Points or 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 or wireless controller.

	`no service mint silence`
no service mint silence	Disables LEDs on Brocade Mobility 300 Access Points or a specified device in the WLAN. It also resets the CLI table expand and MiNT protocol configurations. • mint – Resets MiNT protocol configurations. Disables ping and traceroute parameters • silence – Disables MiNT echo messaging and tracing of route packets

	`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 or wireless controller.

	`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, 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, 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#

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
debug	Disables debug commands
logging	Modifies message logging settings
page	Resets wireless 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

page

Privileged Exec Mode Commands

Toggles wireless 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
page
```

Parameters

None

Example

```
rfs7000-37FABE#page
rfs7000-37FABE#
```

Related Commands:

no	Disables wireless 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

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

Parameters

```
ping <IP/HOSTNAME> {count <1-10000>|dont-fragment|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	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.
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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
pwd
```

Parameters

None

Example

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

rfs7000-37FABE#dir
Directory of flash:/.

  drwx             Fri Aug  3 13:16:52 2012   log
  drwx             Fri Jul  8 15:50:23 2011   Final
  drwx             Mon Jul 18 15:16:35 2011   cache
  drwx             Thu Jul 19 08:40:19 2012   crashinfo
  drwx             Fri Aug  3 13:14:11 2012   archived_logs
  drwx             Sat Jan  1 05:30:25 2000   hotspot
  drwx             Sat Jan  1 05:30:09 2000   floorplans
  drwx             Wed May  9 20:18:19 2012   startuplog
  -rw-   244736    Thu Aug 16 10:05:58 2012   out.tar

rfs7000-37FABE#
```

re-elect

Privileged Exec Mode Commands

Re-elects tunnel wireless controller

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 tunnel wireless controller
<WORD> {on <DEVICE-NAME>}	Optional. Re-elects tunnel wireless controller on all devices whose preferred tunnel wireless controller name matches <WORD> • on <DEVICE-NAME> – Optional. Re-elects tunnel wireless controller on a specified device • <DEVICE-NAME> – Specify the name of the AP or wireless controller.
on <DEVICE-NAME>	Optional. Re-elects tunnel wireless controller on a specified device • <DEVICE-NAME> – Specify the name of the AP or wireless controller.

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 an AP, wireless controller, or RF Domain. Halts a system and performs a warm reboot • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, 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 an a specified device • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, 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 wireless 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, or RF Domain.

Example

```
rfs7000-37FABE#reload force on rfs7000-37FABE
rfs7000-37FABE#
```

remote-debug

Privileged Exec Mode Commands

Troubleshoots remote systems

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
remote-debug
[clear-crashinfo|copy-crashinfo|copy-smartrf-report|copy-techsupport|
          end-session|  live-pktcap|more|offline-pktcap|wireless]

remote-debug [clear-crashinfo|copy-crashinfo|copy-techsupport|
live-pktcap|more|
          offline-pktcap|wireless] [hosts <REMOTE-DEVICE-NAME>|rf-domain
<RF-DOMAIN-NAME>]
          write <URL>

remote-debug copy-smartrf-report rf-domain <RF-DOMAIN-NAME> write <URL>

remote-debug end-session
[copy-crashinfo|copy-smartrf-report|copy-techsupport|
          live-pktcap|more|offline-pktcap|wireless]
```

Parameters

```
remote-debug [clear-crashinfo|copy-crashinfo|copy-techsupport|
live-pktcap|more|
offline-pktcap|wireless] [hosts <REMOTE-DEVICE-NAME>|rf-domain
<RF-DOMAIN-NAME>]
write <URL>
```

remote-debug	Invokes remote system debugging commands
clear-crashinfo	Clears crash info files on a remote system
copy-crashinfo	Copies all crash info files from /flash/crashinfo
copy-techsupport	Copies extensive system information useful to technical support for troubleshooting
live-pktcap	Enables live packet capture
more	Displays contents of a file
offline-pktcap	Captures packets and transfers packet capture data upon completion
wireless	Captures wireless debug messages
hosts <REMOTE-DEVICE-NAME>	Performs selected action on specified remote device(s) • <REMOTE-DEVICE-NAME> – Specify remote system's name (or multiple names separated by space).
rf-domain <RF-DOMAIN-NAME>	Performs selected actions on a specified RF Domain • <RF-DOMAIN-NAME> – Specify the RF Domain name.
write <URL>	Copies the selected information to a directory • <URL> – Specify the directory path in the following format: tftp://<hostname|IP>[:port]/path/ ftp://<user>:<passwd>@<hostname|IP>[:port]/path/ usb1:/path usb2:/path cf:/path

```
remote-debug copy-smartrf-report rf-domain <RF-DOMAIN-NAME> write <URL>
```

remote-debug	Invokes remote system debugging commands
copy-smartrf-report	Copies Smart RF report
rf-domain <RF-DOMAIN-NAME>	Copies Smart RF report for a specified RF Domain • <RF-DOMAIN-NAME> – Specify the RF Domain name.
write <URL>	Copies the selected information to a directory • <URL> – Specify the directory path in the following format: tftp://<hostname|IP>[:port]/path/ ftp://<user>:<passwd>@<hostname|IP>[:port]/path/ usb1:/path usb2:/path cf:/path

```
remote-debug end-session
[copy-crashinfo|copy-smartrf-report|copy-techsupport|
live-pktcap|more|offline-pktcap|wireless]
```

remote-debug	Invokes remote system debugging commands
end-session	Ends an in-progress debugging session

Example

```
rfs7000-37FABE#remote-debug clear-crashinfo hosts 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

```
rfs7000-37FABE#dir
Directory of flash:/.

  drwx             Wed Mar 21 14:19:34 2012   log
  drwx             Fri Jul  8 10:20:23 2011   test
  drwx             Mon Jul 18 09:46:35 2011   cache
  drwx             Tue Mar 20 10:11:09 2012   crashinfo
  drwx             Wed Mar 21 14:24:00 2012   testdir
  drwx             Sat Jan  1 00:00:25 2000   hotspot
  drwx             Sat Jan  1 00:00:09 2000   floorplans
  drwx             Mon Mar 19 13:57:43 2012   startuplog
  -rw-   373760    Thu Mar 15 12:15:07 2012   out.tar

rfs7000-37FABE#

rfs7000-37FABE#rename flash:/test/ Final
rfs7000-37FABE#dir
Directory of flash:/.

  drwx             Wed Mar 21 14:19:34 2012   log
  drwx             Fri Jul  8 10:20:23 2011   Final
  drwx             Mon Jul 18 09:46:35 2011   cache
  drwx             Tue Mar 20 10:11:09 2012   crashinfo
  drwx             Wed Mar 21 14:24:00 2012   testdir
  drwx             Sat Jan  1 00:00:25 2000   hotspot
  drwx             Sat Jan  1 00:00:09 2000   floorplans
  drwx             Mon Mar 19 13:57:43 2012   startuplog
  -rw-   373760    Thu Mar 15 12:15:07 2012   out.tar

rfs7000-37FABE#
```

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
rmdir <DIR>
```

Parameters

```
rmdir <DIR>
```

rmdir <DIR>	Specifies the directory name The directory, specified by the <DIR> parameter, is removed from the file system.

Example

```
rfs7000-37FABE#dir
Directory of flash:/.

  drwx             Wed Mar 21 14:19:34 2012   log
  drwx             Fri Jul  8 10:20:23 2011   Final
  drwx             Mon Jul 18 09:46:35 2011   cache
  drwx             Tue Mar 20 10:11:09 2012   crashinfo
  drwx             Wed Mar 21 14:24:00 2012   testdir
  drwx             Sat Jan  1 00:00:25 2000   hotspot
  drwx             Sat Jan  1 00:00:09 2000   floorplans
  drwx             Mon Mar 19 13:57:43 2012   startuplog
  -rw-   373760    Thu Mar 15 12:15:07 2012   out.tar

rfs7000-37FABE#

rfs7000-37FABE#dir
Directory of flash:/.

  drwx             Wed Mar 21 14:19:34 2012   log
  drwx             Fri Jul  8 10:20:23 2011   Final
  drwx             Mon Jul 18 09:46:35 2011   cache
  drwx             Tue Mar 20 10:11:09 2012   crashinfo
  drwx             Sat Jan  1 00:00:25 2000   hotspot
  drwx             Sat Jan  1 00:00:09 2000   floorplans
  drwx             Mon Mar 19 13:57:43 2012   startuplog
  -rw-   373760    Thu Mar 15 12:15:07 2012   out.tar

rfs7000-37FABE#
```

self

Privileged Exec Mode Commands

Enters the logged device's configuration context

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 of 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:
rfs4000-880DA7>
```

telnet

Privileged Exec Mode Commands

Opens a Telnet session between two network devices

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 out of the other device's context, use the command relevant to that device.

Example

```
rfs7000-37FABE#telnet 172.16.10.4

Entering character mode
Escape character is '^]'.


Brocade Mobility RFS6000 release 5.2.6.0-014D
rfs6000-380649 login: admin
Password:
rfs6000-380649>
```

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 AP or wireless controller • <DEVICE-NAME> – Specify the name of the AP or wireless controller.

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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#
```

Chapter

4

Global Configuration Commands

In this chapter

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 example below describes the process of entering the global configuration mode from the privileged EXEC mode:

```
rfs7000-37FABE# configure terminal
rfs7000-37FABE(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.

```
rfs7000-37FABE(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
  br300                       Configure an br300
  br650                       BR650 access point
  br6511                      BR6511 access point
  br71xx                      BRP71XX 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
  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
  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                            .
  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
  rf-domain                     Create a RF Domain or enter rf-domain context
                                for one or more rf-domains
  rfs4000                       RFS4000 wireless controller
  rfs6000                       RFS6000 wireless controller
  rfs7000                       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-rf-policy               Configure a Smart-RF policy
  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

rfs7000-37FABE(config)#
```

Global Configuration Commands

Table 3 summarizes Global Configuration commands.

TABLE 3 Global Config Commands

Command	Description	Reference
aaa-policy	Configures a AAA policy	*page 4-121*
aaa-tacacs-policy	Configures AAA-TACACS policy	*page 4-122*
advanced-wips-policy	Configures an advanced WIPS policy	*page 4-123*
br300	Adds an Brocade Mobility 300 Access Point to the network, and creates a general profile for the access point	*page 4-124*
br650	Adds an Brocade Mobility 650 Access Point to the network	*page 4-124*
br6511	Adds an Brocade Mobility 6511 Access Point to the network	*page 4-125*
br71xx	Adds an Brocade Mobility 71XX Access Point to the network	*page 4-126*
association-acl-policy	Configures an association ACL policy	*page 4-126*
auto-provisioning-policy	Configures an auto provisioning policy	*page 4-127*
captive portal	Configures a captive portal	*page 4-128*
clear	Clears the event history	*page 4-147*
customize	Customizes the CLI command summary output	*page 4-148*
device	Specifies configuration on multiple devices	*page 4-156*
device-categorization	Configures a device categorization object	*page 4-157*
dhcp-server-policy	Configures a DHCP server policy	*page 4-161*
For more information on DHCP policy, see Chapter 13, DHCP-Server-Policy.	Configures a DNS whitelist	*page 4-162*
do	Runs commands from the EXEC mode	*page 4-165*
event-system-policy	Configures an event system policy	*page 4-175*
firewall-policy	Configures a firewall policy	*page 4-187*
host	Sets the system's network name	*page 4-188*
inline-password-encryption	Stores the encryption key in the startup configuration file	*page 4-188*
ip	Configures *Internet Protocol* (IP) components	*page 4-189*
For more information on Access Control Lists, see Chapter 12, Access-list.	Configures *Layer 2 Tunneling Protocol Version 3* (L2TPV3) tunnel policy	*page 4-190*
mac	Configures MAC access lists (goes to the MAC *Access Control List* (ACL) mode)	*page 4-191*
For more information on Access Control Lists, see Chapter 12, Access-list.	Configures a management policy	*page 4-192*

TABLE 3 Global Config Commands

Command	Description	Reference
For more information on Management policy configuration, see Chapter 16, Management-Policy.	Configures meshpoint related configuration commands	*page 4-193*
For more information on Meshpoint configuration, see Chapter 28, Meshpoint	Configures a set of parameters that defines the *quality of service* (QoS)	*page 4-194*
mint-policy	Configures a MiNT security policy	*page 4-196*
For more information on MiNT policy configuration, see Chapter 15, Mint-Policy.	Configures a network ACL	*page 4-196*
no	Negates a command or sets its default	*page 4-200*
password-encryption	Enables password encryption	*page 4-205*
profile	Configures profile related commands	*page 4-206*
radio-qos-policy	Configures a radio qos policy	*page 4-209*
radius-group	Configures a RADIUS group	*page 4-209*
radius-server-policy	Configures a RADIUS server policy	*page 4-210*
radius-user-pool-policy	Configures a RADIUS user pool policy	*page 4-211*
rf-domain	Creates an RF Domain	*page 4-212*
rfs4000	Adds an Brocade Mobility RFS4000 to the network	*page 4-228*
rfs6000	Adds an Brocade Mobility RFS6000 to the network	*page 4-228*
rfs7000	Adds an Brocade Mobility RFS7000 to the network	*page 4-229*
role-policy	Configures a role policy	*page 4-229*
routing-policy	Configures a routing policy	*page 4-230*
self	Displays a logged device's configuration context	*page 4-231*
smart-rf-policy	Configures a Smart RF policy	*page 4-232*
wips-policy	Configures a WIPS policy	*page 4-233*
wlan	Configures a wireless WLAN	*page 4-234*
wlan-qos-policy	Configures a WLAN QoS policy	*page 4-273*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
end	Ends and exits current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends current mode and moves to the previous mode	*page 5-277*
help	Displays interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*

TABLE 3 Global Config Commands

Command	Description	Reference
service	Invokes service commands to troubleshoot or debug (`config-if`) instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes information to memory or terminal	*page 5-310*

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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-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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 27, .*

advanced-wips-policy

Global Configuration Commands

Configures advanced a *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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

For more information on WIPS, see *Chapter 10, Advanced-WIPS-Policy*.

br300

Global Configuration Commands

Adds an Brocade Mobility 300 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

Syntax:

```
br300 {<MAC}
```

Parameters

```
br300 {<MAC>}
```

<MAC>	Optional. Specify the Brocade Mobility 300 Access Point's MAC address. When this command is issued without any parameters, the default Brocade Mobility 300 Access Point profile is configured.

Example

```
rfs7000-37FABE(config)#br300 11-22-33-44-55-66 ?
rfs7000-37FABE(config-br300-11-22-33-44-55-66)#

rfs7000-37FABE(config)#show wireless ap configured
+-----+----------------+--------------------+-----------------+--------
| IDX |       NAME     |         MAC        |     PROFILE     |  RF-DOMAIN  |
+-----+----------------+--------------------+-----------------+--------
| 1   | br7131-889EC4  | 00-15-70-88-9E-C4  | default-br7131  | default
|
| 2   | br300-445566   | 11-22-33-44-55-66  | default-br300   | default    |
+-----+----------------+--------------------+-----------------+--------
rfs7000-37FABE(config)#
```

Related Commands:

no	Removes an Brocade Mobility 300 Access Point from the network

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

Syntax:

```
br650 <MAC>
```

Parameters

```
br650 <MAC>
```

<MAC>	Specify the Brocade Mobility 650 Access Point's MAC address.

Example

```
rfs7000-37FABE(config)#br650 11-22-33-44-55-66 ?
rfs7000-37FABE(config-device-11-22-33-44-55-66)

rfs7000-37FABE(config)#show wireless ap configured
+-----+----------------+--------------------+------------------+--------
| IDX |       NAME     |         MAC        |     PROFILE      |  RF-DOMAIN  |
+-----+----------------+--------------------+------------------+--------
| 1   | br7131-889EC4   | 00-15-70-88-9E-C4   | default-br7131   | default
|
| 2   | br650-445566    | 11-22-33-44-55-66   | default-br650    | default     |
+-----+----------------+--------------------+------------------+--------
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

Syntax:

```
br6511 <MAC>
```

Parameters

```
br6511 <MAC>
```

<MAC>	Specify the Brocade Mobility 6511 Access Point's MAC address.

Example

```
rfs7000-37FABE(config)#br6511 00-17-70-88-9E-C4 ?
rfs7000-37FABE(config-device-00-17-70-88-9E-C4)#
```

Related Commands:

no	Removes an Brocade Mobility 6511 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

Syntax:

```
br71xx <MAC>
```

Parameters

```
br71xx <MAC>
```

<MAC>	Specify the Brocade Mobility 71XX Access Point's MAC address.

Example

```
rfs7000-37FABE(config)#br71xx 00-15-70-88-9E-C4
rfs7000-37FABE(config-device-00-15-70-88-9E-C4)#
```

Related Commands:

no	Removes an Brocade Mobility 71XX Access Point 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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

  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,* .

captive portal

Global Configuration Commands

A captive portal provides secure guest access and authentication services to the network. Table 10 lists the command to enter the captive portal configuration mode.

TABLE 4 Captive-Portal Config Commands

Command	Description	Reference
captive-portal	Creates a new captive portal and enters its configuration mode	*page 4-128*
captive-portal-mode commands	Summarizes captive portal configuration commands	*page 4-130*

captive-portal

captive portal

Configures a captive portal

Supported in the following platforms:

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

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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
  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
  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

Table 5 summarizes captive portal configuration mode commands.

TABLE 5 Captive-Portal-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 4-130*
access-type	Configures a captive portal's access type	*page 4-131*
accounting	Enables a captive portal's accounting records	*page 4-132*
connection-mode	Configures a captive portal's connection mode	*page 4-133*
custom-auth	Configures custom user information	*page 4-134*
data-limit	Enforces data limit on captive portal clients	*page 4-134*
inactivity-timeout	Defines an inactivity timeout in seconds	*page 4-135*
logout-fqdn	Clears the logout FQDN address	*page 4-136*
no	Resets or disables captive portal commands	*page 4-136*
server	Configures the captive portal server parameter	*page 4-140*
simultaneous-users	Specifies a username used by a MAC address pool	*page 4-141*
terms-agreement	Enforces the user to agree to terms and conditions (included in login page) for captive portal access	*page 4-141*
use	Defines captive portal configuration settings	*page 4-142*
webpage	Configures captive portal Web page parameters	*page 4-143*
webpage-auto-upload	Enables automatic upload of advanced Web pages on a captive portal	*page 4-145*
webpage-location	Specifies the location of Web pages used for captive portal authentication	*page 4-146*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
do	Runs commands from the EXEC mode	*page 4-165*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes information to memory or terminal	*page 5-310*

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
access-time <30-10080>
```

Parameters

```
access-time <30-10080>
```

<30-10080>	Defines the access time allowed for a wireless client from 30 - 10080 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	Removes the permitted access time for a client

access-type

captive-portal-mode commands

Defines the captive portal access type

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
access-type [custom-auth-radius|logging|no-auth|radius|self-registration]

access-type self-registration user-pool <RAD-USER-POOL-NAME> group-name
<GROUP-NAME>
```

Parameters

```
access-type [custom-auth-radius|logging|no-auth|radius]
```

custom-auth-radius	Verifies custom user information for authentication (RADIUS lookup of given information, such as name, e-mail address, telephone etc.)
logging	Generates a logging record of users and allowed access

no-auth	Defines no authentication required for a guest (guest is redirected to welcome message)
radius	Enables RADIUS authentication for wireless clients

```
access-type self-registration user-pool <RAD-USER-POOL-NAME> group-name
<GROUP-NAME>
```

self-registration	Allows guest self registration once redirected to the login page
user-pool <RAD-USER-POOL-NAME>	Specifies the RADIUS user pool to which the self registered user is added • <RAD-USER-POOL-NAME> – Specify the RADIUS user pool name.
group-name <GROUP-NAME>	Specifies the group, within the specified user pool, to which the self registered user is added • <GROUP-NAME> – Specify the group name.

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

accounting

captive-portal-mode commands

Enables accounting records for a captive portal

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
accounting [radius|syslog]

accounting radius

accounting syslog host <IP/HOSTNAME> {port <1-65535>}
```

Parameters

```
accounting radius
```

radius	Enables support for RADIUS accounting messages

```
accounting syslog host <IP/HOSTNAME> {port <1-65535>}
```

syslog host <IP/HOSTNAME>	Enables support for syslog accounting messages • 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.

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

connection-mode

captive-portal-mode commands

Configures a captive portal's connection mode. HTTP uses plain unsecured connection for user requests. HTTPS uses encrypted connection to support user requests.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
connection-mode [http|https]
```

Parameters

```
connection-mode [http|https]
```

http	Sets HTTP as the default connection mode
https	Sets HTTPS as the default connection mode 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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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@example.com

rfs7000-37FABE(config-captive-portal-test)#show context
captive-portal test
 access-type logging
 access-time 35
 custom-auth info bob,\ bob@example.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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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.

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,\ bobexample.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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 disables captive portal mode commands or resets parameters to their default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
no
[access-time|access-type|accounting|connection-mode|custom-auth|data-limit|
          inactivity-timeout|logout-fqdn|
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|simultaneous-users|terms-agreement|webpage-auto-upload|
          webpage-location]

no accounting [radius|syslog]

no custom-auth info

no server host
no server mode {centralized-controller [hosting-vlan-interface]}

no use [aaa-policy|dns-whitelist]

no webpage external [agreement|fail|login|welcome]
no webpage internal [org-name|org-signature]
no webpage internal [agreement|fail|login|welcome]
[description|footer|header|
          main-logo|small-logo|title]
```

Parameters

```
no [access-time|access-type|connection-mode|data-limit|inactivity-timeout|
logout-fqdn|
simultaneous-users|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 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 agreement requirement 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 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 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 [agreement|fail|login|welcome]`
no webpage external	Resets the configuration of external Web pages displayed when a user interacts with the captive portal
agreement	Resets the agreement page
fail	Resets the fail page
login	Resets the login page
welcome	Resets the welcome page

	`no webpage internal [org-name|org-signature]`
no webpage external	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 [agreement|fail|login|welcome] [description|footer|header|main-logo|small-logo|title]`
no webpage external	Resets the configuration of internal Web pages displayed when a user interacts with the captive portal
agreement	Resets the agreement page
fail	Resets the fail page
login	Resets the login page
welcome	Resets the welcome page

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@example.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@example.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
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
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	Configures 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
aaa-policy	Configures a AAA policy
For more information on DHCP policy, see Chapter 13, DHCP-Server-Policy.	Configures a DNS whitelist

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
server [host|mode]

server host <IP/HOSTNAME>

server mode [centralized|centralized-controller
{hosting-vlan-interface}|self]
```

Parameters

```
server host <IP/HOSTNAME>
```

host <IP/HOSTNAME>	Configures the internal captive portal authentication server (wireless controller or access point) • <IP/HOSTNAME> – Specify the IP address or hostname of the captive portal server. For centralized wireless controller mode, this should be a virtual hostname and not IP address.

```
server mode [centralized|centralized-controller
{hosting-vlan-interface}|self]
```

mode	Configures the captive portal server mode
centralized	Considers the configured server hostname or IP address as the centralized captive portal server
centralized-controller {hosting-vlan-interface}	Uses the configured hostname as the virtual captive portal server name across wireless controllers • hosting-vlan-interface – Optional. Configures the VLAN where the client can reach the wireless controller (server)
self	Selects the captive portal server as the same device supporting the WLAN

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@example.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

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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@example.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 guest access

Supported in the following platforms:

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

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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@example.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 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,* .

For more information on DNS whitelists, see *Chapter 4, For more information on DHCP policy, see Chapter 13, DHCP-Server-Policy..*

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 configure servers for the captive portal. • <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 URL access. • <DNS-WHITELIST-NAME> – Specify the DNS whitelist name.

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@example.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
For more information on DHCP policy, see Chapter 13, DHCP-Server-Policy.	Configures a DNS whitelist
aaa-policy	Configures a AAA policy

webpage

captive-portal-mode commands

Configures Web pages displayed when interacting with a captive portal. There are four (4) different pages.

- 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 to use the captive portal.
- login – This page is displayed when the user connects to the captive portal. It fetches login credentials from the user.
- 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 wireless controller or an external location.

Supported in the following platforms:

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

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
webpage [external|internal]

webpage external [agreement|fail|login|welcome] <URL>

webpage internal [agreement|fail|login|org-name|org-signature|welcome]
webpage internal [org-name|org-signature] <LINE>
webpage internal [agreement|fail|login|welcome] [description|footer|
header|title]
          <CONTENT>
webpage internal [agreement|fail|login|welcome] [main-logo|small-logo] <URL>
```

Parameters

```
webpage external [agreement|fail|login|welcome] <URL>
```

external	Indicates Web pages being served are external to the captive portal
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 getting user credentials
welcome	Indicates the page is displayed after a user has been successfully authenticated
<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_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_mc=WING_TAG_AP_MAC. Use '&' or '?' character to separate field-value pair. Note: Enter 'ctrl-v' followed by '?' to configure query string

```
webpage internal [agreement|fail|login|welcome]
[description|footer|header|title] <CONTENT>
```

internal	Indicates the Web pages are internal
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
welcome	Indicates the page is displayed after a user has been successfully authenticated
description	Indicates the content is the description portion of each internal, agreement, fail, and welcome page
footer	Indicates the content is the footer portion of each internal, agreement, fail, 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 internal, agreement, fail, and welcome page. The header portion contains the heading information for each of these pages.

title	Indicates the content is the title of each internal, agreement, fail, and welcome page. The title for each of these pages is configured here.
<CONTENT>	Specify the content displayed for each of the different components of the Web page. Enter up to 900 characters for the description and 256 characters each for header, footer, and title.

`webpage internal [agreement|fail|login|welcome] [main-logo|small-logo] <URL>`

internal	Indicates the Web pages are internal
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
welcome	Indicates the page is displayed after a user has been successfully authenticated
main-logo	Indicates the main logo displayed in the header portion of each Web page
small-logo	Indicates the logo image displayed in the footer portion of each Web page, and constitutes the organization’s signature
<URL>	Indicates the complete URL of the main-log and small-logo files

`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.example.com

rfs7000-37FABE(config-captive-portal-test)#show context
captive-portal test
 access-time 35
 custom-auth info bob,\ bob@example.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.example.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

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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-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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 wireless controller
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@example.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 location settings
webpage	Configures a captive portal's Web page (login, welcome, fail, and terms) settings

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
clear event-history
```

Parameters

```
clear event-history
```

event-history	Clears the event history file

Example

```
rfs7000-37FABE(config)#show event-history
EVENT HISTORY REPORT
Generated on '2012-06-21 17:41:31 IST' by 'admin'

2012-06-21 17:41:19     rfs7000-37FABE  SYSTEM     LOGIN
Successfully logged in User: 'admin' with privilege 'superuser' from 'ssh'
2012-06-21 16:39:26    br7131-4AA708  SYSTEM    UI_USER_AUTH_SUCCESS UI User:
'admin', from: '172.16.10.105' authentication successful
2012-06-21 16:39:23     br7131-4AA708  SYSTEM     LOGOUT              Logged
out User: 'admin' with privilege 'superuser' from '172.16.10.12'
```

```
2012-06-21 16:39:11    br7131-4AA708  SYSTEM    UI_USER_AUTH_FAIL    UI User:
'admin', from: '172.16.10.105' authentication failed
2012-06-21 16:38:22     br7131-4AA708  SYSTEM     LOGOUT               Logged
out User: 'admin' with privilege 'superuser' from '172.16.10.105(web)'
2012-06-21 16:37:35     rfs7000-37FABE  DIAG       NEW_LED_STATE        LED
state message --More-
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#clear event-history

rfs7000-37FABE(config)#show event-history
EVENT HISTORY REPORT
Generated on '2012-06-21 17:42:26 IST' by 'admin'

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 (ap-name <1-64>, auth, bss, enc, hostname
<1-64>, ip,
          last-active, location <1-64>, mac, radio-alias <3-67>, radio-id,
radio-type, 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 (ap-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 (ap-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 (ap-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|ap-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-throughput)

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 (ap-name <1-64>,auth,bss,enc,hostname
<1-64>,ip,
last-active,location <1-64>,mac,radio-alias <3-67>,radio-id,radio-type,state,
username <1-64>,vendor,vlan,wlan)
```

show-wireless-client	Customizes the show wireless client command output
ap-name <1-64>	Includes the ap-name column, which displays the name of the AP with which this client associates • <1-64> – Sets the ap-name column width from 1 - 64 characters
auth	Includes the auth column, which displays the authorization protocol used by the wireless client
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
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 (average-retry-number,error-rate, hostname <1-64>,mac,noise,q-index,rx-rate,signal,snr,t-index,tx-rate)`
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 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 (ap-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
ap-mac	Includes the ap-name column, which displays the AP's MAC address in the AA-BB-CC-DD-EE-FF format. Applicable only in case of non-wireless controller meshpoint
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 meshpoint • <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 (ap-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
ap-name <1-64>	Includes the ap-name column, which displays name of the AP reporting a neighbor • <1-64> – Sets the ap-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 (ap-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
ap-name <1-64>	Includes the ap-name column, which displays name of the AP reporting a neighbor • <1-64> – Sets the ap-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 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,ap-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
ap-name <1-64>	Includes the ap-name column, which displays information about the AP this radio belongs • <1-64> – Sets the ap-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 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 ap-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 cutomized 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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
device {containing|filter}

device containing <STRING> {filter type [br650|br6511|
          br71xx|rfs4000|rfs6000|rfs7000]}

device filter type [br650|br6511|br71xx|rfs4000|
          rfs6000|   rfs7000|]
```

Parameters

```
device containing <STRING> {filter type [br650|br6511|
br71xx|rfs4000|rfs6000|rfs7000]}
```

device	Configures a basic device profile
containing <STRING>	Configures the search string to search for in the device's hostname. Only those devices that have the search string in their hostname can be configured. • <STRING> – Specify the string to search for in the hostname of the devices
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
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|br71xx|
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

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 ap filter type br71xx
% Error: Parsing cmd line (1)
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#device containing ap 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. Table 6 lists the command to enter the device categorization configuration mode.

TABLE 6 Device-Categorization Config Command

Command	Description	Reference
device-categorization	Creates a device categorization list and enters its configuration mode	*page 4-157*
device-categorization-mode commands	Summarizes device categorization list configuration mode commands	*page 4-158*

device-categorization

device-categorization

Configures a device categorization list. This list categorizes devices as sanctioned or neighboring. This information determines which devices are allowed access to the network and which are unsanctioned devices.

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

Table 7 summarizes device categorization configuration commands.

TABLE 7 Device-Categorization-Mode Commands

Command	Description	Reference
mark-device	Adds a device to the device categorization list	*page 4-159*
no	Removes a device from the device categorization list	*page 4-160*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
do	Runs commands from the EXEC mode	*page 4-165*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 5-283*

TABLE 7 Device-Categorization-Mode Commands

Command	Description	Reference
show	Displays running system information	*page 6-315*
write	Writes information to memory or terminal	*page 5-310*

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
mark-device <1-1000> [sanctioned|neighboring] [ap|client]
mark-device <1-1000> [sanctioned|neighboring] ap {mac <MAC>|ssid <SSID> {mac <MAC>}}
mark-device <1-1000> [sanctioned|neighboring] client {mac <MAC>}
```

Parameters

```
mark-device <1-1000> [sanctioned|neighboring] ap {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.
ap {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. 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
ap
 mac 11-22-33-44-55-66
```

```
rfs7000-37FABE(config-device-categorization-rfs7000)#show context
device-categorization rfs7000
 mark-device 1  sanctioned ap mac 11-22-33-44-55-66
rfs7000-37FABE(config-device-categorization-rfs7000)#
```

Related Commands:

no	Removes a device 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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
no mark-device <1-1000> [neighboring|sanctioned] [ap|client]
no mark-device <1-1000> [sanctioned|neighboring] client {mac <MAC>}
no mark-device <1-1000> [sanctioned|neighboring] ap {mac <MAC>|ssid <SSID>
{mac <MAC>}}
```

Parameters

```
no mark-device <1-1000> [sanctioned|neighboring] ap {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
ap {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 ap mac 11-22-33-44-55-66
rfs7000-37FABE(config-device-categorization-rfs7000)#

rfs7000-37FABE(config-device-categorization-rfs7000)#no mark-device 1
sanctioned  ap 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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

For more information on DHCP policy, see *Chapter 13, DHCP-Server-Policy*.

dns-whitelist

Global Configuration Commands

Configures a whitelist of devices permitted access to the network or captive portal. Table 8 lists DNS Whitelist configuration mode commands.

TABLE 8 DNS-Whitelist Config Commands

Command	Description	Reference
dns-whitelist	Creates a DNS whitelist and enters its configuration mode	*page 4-162*
dns-whitelist-mode commands	Summarizes DNS whitelist configuration mode commands	*page 4-163*

dns-whitelist

For more information on DHCP policy, see Chapter 13, DHCP-Server-Policy.

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 a DNS Whitelist

dns-whitelist-mode commands

For more information on DHCP policy, see Chapter 13, DHCP-Server-Policy.

Table 9 summarizes DNS white list configuration mode commands.

TABLE 9 DNS-Whitelist-Mode Commands

Command	Description	Reference
permit	Permits a host, existing on a DNS whitelist, access to the network or captive portal	*page 4-163*
no	Negates a command or reverts to default	*page 4-164*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
do	Runs commands from the EXEC mode	*page 4-165*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 5-283*
show	Displays running system information	*page 6-319*
write	Writes information to memory or terminal	*page 5-310*

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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.
suffix	Optional. Matches any hostname including the specified name as suffix

Example

```
rfs7000-37FABE(config-dns-whitelist-test)#permit example.com suffix

rfs7000-37FABE(config-dns-whitelist-test)#show context
dns-whitelist test
permit example.com suffix
rfs7000-37FABE(config-dns-whitelist-test)#
```

Related Commands:

no	Resets or disables DNS whitelist commands

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 example.com suffix
rfs7000-37FABE(config-dns-whitelist-test)#

rfs7000-37FABE(config-dns-whitelist-test)#no permit example.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

do

Global Configuration Commands

Use the do command to run commands from the EXEC mode. These commands perform tasks, such as clearing caches, setting device clock, upgrades etc.

Generally, use the do command to execute commands from the Privilege Executable or User Executable modes.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
do [ap-upgrade|archive|boot|cd|change-passwd|clear|clock|cluster|commit|
configure|
          connect|copy|create-cluster|crypto|debug|delete|diff|dir|disable|
edit|     enable|erase|
          format|halt|help|join-cluster|l2tpv3|logging|mint|mkdir|more|no|
page|ping|pwd|
          re-elect|reload|remote-debug|rename|revert|rmdir|self|ssh|telnet|
terminal|  time-it|
          traceroute|upgrade|upgrade-abort|
watch|write|clrscr|exit|service|show]

do ap-upgrade [<DEVICE-NAME>|all|br650|br71xx|
          load-image|rf-domain|cancel-upgrade]

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

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

do cd {<DIR>}

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

do clear
[arp-cache|cdp|counters|crypto|event-history|firewall|ip|lldp|spanning-tree|
          vrrp]
```

```
do clock set <TIME> <DAY> <MONTH> <YEAR>

do clrscr

do cluster start-election

do commit write memory

do configure [terminal|self]

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

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

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

do crypto [key|pki]

do delete /force /recursive <FILE>

do diff [<FILE1>|<URL1>] [<FILE2>|<URL2>]

do dir {/all} {/recursive} {<DIR>} {all-filesystems}

do edit <FILE>

do erase [cf:|flash:|nvram:|startup-config|usb1:|usb2:]

do exit

do format cf:

do halt {on <DEVICE>}

do help {search|show}

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

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

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

do mint [ping|security|traceroute]
do mint ping <MINT-ID> {count <1-10000>|size <1-64000>|timeout <1-10>}
do mint traceroute <MINT-ID> {destination-port <1-65535>|max-hops <1-255>|
          source-port <1-65535>|timeout <1-255>}
do mint security [approve-request [<MAC>|all]|create-security-trustpoint]

do mkdir <DIR>

do more <FILE>

do no [adoption|captive-portal|crypto|debug|logging|page|service|terminal|
          upgrade|wireless]
```

```
do page

do ping <IP/HOSTNAME>

do pwd

do re-elect tunnel-controller {<WORD> {on <DEVICE-NAME>}|on <DEVICE-NAME>}

do reload {cancel|force|in|on}

do rename <FILE>

do revert

do rmdir <DIR>

do self

do service
[advanced-wips|br300br300|clear|cli-tables-expand|cli-tables-skin|cluster|
copy|
          delete-offline-aps|force-send-config|load-balancing|locator|mint|
pktcap|pm| radio|
          radius|set|signal|smart-rf|ssm|start-shell|trace|wireless|show]

do show
[adoption|advanced-wips|ap-upgrade|boot|captive-portal|cdp|clock|cluster|

commands|context|critical-resources|crypto|debug|debugging|device-categorizat
ion|
          dot1x|eval|
event-history|event-system-policy|file|firewall|interface|ip|
          ip-access-list-stats|
l2tpv3|licenses|lldp|logging|mac-access-list-stats|
          mac-address-table|mint|
noc|ntp|password-encryption|power|pppoe-client|privilege|
          reload|remote-debug|
rf-domain-manager|role|route-maps|rtls|running-config|
          session-changes|session-config|sessions|smart-rf|spanning-tree|
startup-config|
          terminal|timezone|upgrade-status|version|vrrp|what|wireless|wwan]

do ssh <IP>

do telnet <IP/HOSTNAME>

do terminal [length <LINES>|width <CHARACTERS>]

do time-it <CLI-COMMAND>

do traceroute <ARGS>

do upgrade [<FILE>|<URL>]

do upgrade-abort {on <DEVICE>}

do watch <TIME> <CLI-COMMAND>

do write [memory|terminal]
```

Parameters

	`do ap-upgrade [<DEVICE-NAME>|all|br650|br6511|| br71xx|load-image|rf-domain|cancel-upgrade]`
ap-upgrade	Runs the ap-upgrade command For more information on the AP upgrade command, see *ap-upgrade*.
	`do archive tar [/create|/table|/xtract] [<FILE>|<URL>]`
archive	Runs the archive command For more information on the archive command, see *archive*.
	`do boot system [primary|secondary] {on <DEVICE-NAME>}`
boot	Configures the image used for the next boot For more information on the boot command, see *boot*.
	`do cd {<DIR>}`
cd <DIR>	Runs the command to change the present working directory For more information on the cd command see *cd*.
	`do change-passwd {<OLD-PASSWORD>} [<NEW-PASSWORD>]`
change-passwd {<OLD-PASSWORD>} {<NEW-PASSWORD>}	Changes password of the logged user For more information on the clear command, see *change-passwd*.
	`do clear [arp-cache|cdp|counters|crypto|event-history|firewall|ip|lldp|logging| spanning-tree|vrrp]`
clear	Clears configured WLAN settings For more information on the clear command, see *clear*.
	`do clock set <TIME> <DAY> <MONTH> <YEAR>`
clock set <TIME> <DAY> <MONTH> <YEAR>	Sets the device's time and date For more information on the clock command, see *clock*.
	`do clrscr`
clrscr	Clears the current screen For more information on the clrscr command, see *clrscr*.
	`do cluster start-election`
cluster start-election	Starts the configuration for creating a cluster of servers For more information on the cluster command, see *cluster*.
	`do commit writer memory`
commit write memory	Commits the changes made in the current CLI session For more information on the commit command, see *commit*.
	`do configure [terminal|self]`
configure [terminal|self]	Changes the configuration mode For more information on the configure command, see *configure*.

	`do connect [<REMOTE-DEVICE>|mint-id <DEVICE-MINT-ID>]`
connect [<REMOTE-DEVICE>| mint-id <DEVICE-MINT-ID>]	Connects to a remote device to configure it. This command uses a device's hostname or its MiNT ID to connect. For more information on the connect command, see *connect*.

	`do copy [<SOURCE-FILE>|<SOURCE-URL>] [<DESTINATION-FILE>|<DESTINATION-URL>]`
copy [<SOURCE-FILE>| <SOURCE-URL>] [<DESTINATION-FILE>| <DESTINATION-URL>]	Copies a file from one location to another For more information on the copy command, see *copy*.

	`do create-cluster name <CLUSTER-NAME> ip <IP> {level [1|2]}]`
create-cluster name <CLUSTER-NAME> ip <IP> {level [1|2]}]	Creates a new cluster on a specified device For more information on the create-cluster command, see *create-cluster*.

	`do crypto [key|pki]`
crypto [key|pki]	Configures the crypto command For more information on the crypto command, see *crypto*.

	`do delete /force /recursive <FILE>`
delete /force /recursive <FILE>	Deletes a file from the device's file system For more information on the delete command, see *delete*.

	`do diff [<FILE1>|<URL1>] [<FILE2>|<URL2>]`
diff [<FILE1>|<URL1>] [<FILE2>|<URL2>]	Compares two files and displays the difference between them For more information on the diff command, see *diff*.

	`do dir {/all} {/recursive} {<DIR>} {all-filesystems}`
dir {/all} {/recursive} {<DIR>} {all-filesystems}	Displays the content of a directory in the device's file system For more information on the dir command, see *dir*.

	`do erase [cf:|flash:|nvram:|startup-config|usb1:|usb2:]`
do erase [cf:|flash:|nvram:| startup-config|usb1]	Erases the content of the specified storage device. Also erases the startup configuration to restore the device to its default. For more information on the erase command, see *erase*.

	`do exit`
exit	Exits the CLI For more information on the exit command, see *exit*.

	`do format cf:`
format cf:	Formats the CF card installed on the device For more information on the format command, see *format*.

	`do halt {on <DEVICE-NAME>}`
halt {on <DEVICE-NAME>}	Stops the device For more information on the halt command, see *halt*.

	`do help {search|show}`
help {search|show}	Displays the command line interface help For more information on the help command, see *help*.
	`do join-cluster <IP> user <USERNAME> password <WORD> {level [1|2]| mode [active|standby]}`
join-cluster	Adds a wireless controller, as cluster member, to an existing cluster of wireless controllers. For more information on the join-cluster command, see *join-cluster*.
	`do l2tpv3 tunnel [<TUNNEL-NAME>|all]`
l2tpv3 tunnel [<TUNNEL-NAME>|all]	Establishes or brings down a L2TPV3 tunnel For more information on the l2tpv3 command, see *l2tpv3*.
	`do logging monitor {<0-7>|alerts|critical|debugging|emergencies|errors| informational|notification|warnings}`
logging monitor {<0-7>|alerts|critical| debugging|emergencies| errors|informational| notification|warnings}	Configures the logging level for the device For more information on the logging command, see *logging*.
	`do mint [ping|security|traceroute]`
mint [ping|security|traceroute]	Performs MiNT operations such as ping and traceroute For more information on the mint command, see *mint*.
	`do mkdir <DIR>`
mkdir <DIR>	Creates a directory in the device's file structure For more information on the mkdir command, see *mkdir*.
	`do more <FILE>`
more <FILE>	Displays a file in the console window For more information on the more command, see *more*.
	`do no [adoption|captive-portal|crypto|debug|logging|page|service|terminal|upgrade| wireless]`
no [adoption| captive-portal| crypto|debug|page| service| terminal|upgrade| wireless|logging]	Reverts or negates a command For more information on the no command, see the respective profiles and modes.
	`do page`
page	Toggles paging of the command line interface For more information on the page command, see *page*.
	`do ping <IP-HOSTNAME>`
ping <IP>	Pings a device to check its availability For more information on the ping command, see *ping*.

	`do pwd`
pwd	Displays the current working directory For more information on the pwd command, see *pwd*.
	`do re-elect tunnel-controller {<WORD> {on <DEVICE-NAME>}|on <DEVICE-NAME>}`
re-elect tunnel-controller {<WORD> {on <DEVICE-NAME>}| on <DEVICE-NAME>}	Re-elects tunnel wireless controller For more information on the re-elect command, see *re-elect*.
	`do reload {cancel|force|in|on}`
reload {cancel|force|in|on}	Halts the device and performs a warm reboot For more information on the reload command, see *reload*.
	`do rename <FILE>`
rename <FILE>	Renames a file on the device's file system For more information on the rename command, see *rename*.
	`do revert`
revert	Reverts the changes made to the system to their last saved configuration For more information on the revert command, see *revert*.
	`do rmdir <DIR>`
rmdir <DIR>	Removes a directory in the device's file system For more information on the rmdir command, see *rmdir*.
	`do self`
self	Loads the configuration context of the currently logged device For more information on the self command, see *self*.
	`do service <PARAMETER>`
service <PARAMETER>	Performs the different service commands For more information on the service commands, see *service*.
	`do show <PARAMETER>`
show <parameter>	Displays information about the state of device, its configuration, current status, and statistics For more information on the show command, see *show*.
	`do ssh <IP>`
ssh <IP-HOSTNAME>	Connects to a device using the SSH protocol For more information on the SSH command, see *ssh*.
	`do telnet <IP/HOSTNAME>`
telnet <IP/HOSTNAME>	Connects to a device using the Telnet protocol For more information on the Telnet command, see *telnet*.
	`do terminal [length <LINES>|width <CHARACTERS>]`
do terminal [length <LINES>| width <CHARACTERS>]	Configures the CLI display characteristics For more information on the terminal command, see *terminal*.

	`do time-it <CLI-COMMAND>`
time-it <CLI-COMMAND>	Captures the time required to execute a command in the CLI For more information on the time-it command, see *time-it*.
	`do traceroute <ARGS>`
traceroute <ARGS>	Traces the path to the target devices through the network For more information on the traceroute command, see *traceroute*.
	`do upgrade [<FILE>|<URL>]`
upgrade [<FILE>|<URL>]	Upgrades the device's firmware from a file or a defined location For more information on the upgrade command, see *upgrade*.
	`do upgrade-abort` *`{on <DEVICE>}`*
upgrade-abort {on <DEVICE-NAME>}	Aborts an in-progress upgrade on a logged or remote device For more information on the upgrade abort command, see *upgrade-abort*.
	`do watch <TIME> <CLI-COMMAND>`
watch <TIME> <CLI-COMMAND>	Repeats a CLI command at a periodic interval For more information on the watch command, see *watch*.
	`do write [memory|terminal]`
write [memory|terminal]	Writes the changes made to the running configuration to memory or a terminal For more information on the write command, see *write*.

Example

```
rfs7000-37FABE(config)#do ?
  ap-upgrade      AP firmware upgrade
  archive         Manage archive files
  boot            Boot commands
  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.
  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
  format          Format file system
  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
  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
  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
  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
  service         Service Commands
  show            Show running system information

rfs7000-37FABE(config)#
```

Related Commands:

ap-upgrade	Upgrades access point(s)
archive	Runs the archive command
boot	Configures the image used for the next boot
cd	Changes current working directory
change-passwd	Changes current login user's password
clear	Clears specified configurations
clock	Configures a device's time and date
clrscr	Clears the current screen
cluster	Starts the configuration for creating a cluster of servers
commit	Commits changes made in the current CLI session
configure	Changes configuration mode
connect	Configures a remote device (uses the device's hostname or MiNT ID to connect)
copy	Copies a file from one location to another
create-cluster	Creates a new cluster on a specified device
crypto	Invokes crypto commands
delete	Deletes a file from a device's filesystem

diff	Compares two files and displays the difference
dir	Displays the content of a directory in the device's file system
disable	Moves control to the User Exec mode
edit	Edits a file
enable	Moves control to the Privilege Exec mode
erase	Erases content of the specified storage device. Also erases the startup configuration to restore the device to its default settings.
exit	Exits from the CLI
format	Formats the CF card installed on a device
halt	Stops a device
help	Displays CLI help
join-cluster	Adds a wireless controller, as cluster member, to an existing cluster of wireless controllers
l2tpv3	Establishes or brings down a L2TPV3 tunnel
logging	Configures a device's logging
mint	Performs MiNT operations such as ping and traceroute
mkdir	Creates a directory in the device's file structure
more	Displays a file in the console window
no	Reverts or negates a command
page	Toggles paging of the command line interface
ping	Pings a device to check its availability
pwd	Displays the current working directory
re-elect	Re-elects tunnel wireless controller
reload	Halts a device and performs a warm reboot
remote-debug	Troubleshoots remote systems
rename	Renames a file on a device's file system
revert	Reverts changes made to the system during the current CLI session
rmdir	Removes a directory in a device's file system
self	Loads a device's configuration context
service	Executes service commands
ssh	Connects to a device using SSH
show	Displays a device's state, configuration, and statistics
telnet	Uses Telnet to connect to a device
terminal	Sets the number of characters per line, and the number of lines displayed within the terminal window
time-it	Captures the time required to execute a CLI command
traceroute	Traces the path to target devices

upgrade	Upgrades a device's firmware from a file or remote location
upgrade-abort	Aborts an in-progress upgrade on a logged or remote device
watch	Repeats a specified CLI command at periodic intervals
write	Writes changes made in the current session to the memory

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 . Table 10 lists event system configuration mode commands.

TABLE 10 Event-System-Policy Config Command

Command	Description	Reference
event-system-policy	Creates an event system policy and enters its configuration mode	*page 4-175*
event-system-policy-mode commands	Summarizes event system policy configuration mode commands	*page 4-176*

event-system-policy

event-system-policy

Configures a system wide events handling policy

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

Table 11 summarizes event system policy configuration mode commands.

TABLE 11 Event-System-Policy Mode Commands

Command	Description	Reference
event	Configures an event	*page 4-177*
no	Negates a command or reverts to default	*page 4-186*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
do	Runs commands from the EXEC mode	*page 4-165*

TABLE 11 Event-System-Policy Mode Commands

Command	Description	Reference
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes information to memory or terminal	*page 5-310*

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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
  ap              Access Point module
  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             Fwu module
         isdn             Isdn module
  licmgr          License module
  mesh            Mesh module
  mgmt            Management Services
  nsm             Network Services Module
  pm              Process-monitor module
  radconf         Radius Configuration Daemon
  radio           Radio module
  securitymgr     Securitymgr module
  smrt            Smart-rf module
  smtpnot         Smtpnot module
```

```
  system          System module
  test            Test module
  vrrp            Virtual Router Redundancy Protocol
  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 • adv-wips-event-1 – Event adv-wips-event-1 message • adv-wips-event-10 – Event adv-wips-event-10 message • adv-wips-event-105 – Event adv-wips-event-105 message • adv-wips-event-109 – Event adv-wips-event-109 message • adv-wips-event-11 – Event adv-wips-event-11 message • adv-wips-event-110 – Event adv-wips-event-110 message • adv-wips-event-111 – Event adv-wips-event-111 message • adv-wips-event-112 – Event adv-wips-event-112 message • adv-wips-event-113 – Event adv-wips-event-113 message • adv-wips-event-114 – Event adv-wips-event-114 message • adv-wips-event-115 – Event adv-wips-event-115 message • adv-wips-event-116 – Event adv-wips-event-116 message • adv-wips-event-117 – Event adv-wips-event-117 message • adv-wips-event-118 – Event adv-wips-event-118 message • adv-wips-event-119 – Event adv-wips-event-119 message • adv-wips-event-12 – Event adv-wips-event-12 message • adv-wips-event-120 – Event adv-wips-event-120 message • adv-wips-event-121 – Event adv-wips-event-121 message • adv-wips-event-13 – Event adv-wips-event-13 message • adv-wips-event-14 – Event adv-wips-event-14 message • adv-wips-event-142 – Event adv-wips-event-142 message • adv-wips-event-16 – Event adv-wips-event-16 message • adv-wips-event-19 – Event adv-wips-event-19 message • adv-wips-event-2 – Event adv-wips-event-2 message • adv-wips-event-21 – Event adv-wips-event-21message • adv-wips-event-220 – Event adv-wips-event-220 message • adv-wips-event-221 – Event adv-wips-event-221 message • adv-wips-event-222 – Event adv-wips-event-222 message • adv-wips-event-25 – Event adv-wips-event-25 message • adv-wips-event-26 – Event adv-wips-event-26 message • adv-wips-event-29 – Event adv-wips-event-29 message

<event-type>	<event-name>
	• adv-wips-event-3 – Event adv-wips-event-3 message • adv-wips-event-47 – Event adv-wips-event-47 message • adv-wips-event-63 – Event adv-wips-event-63 message • adv-wips-event-87 – Event adv-wips-event-87 message
ap	Configures AP event messages • adopted – Event AP adopted message • adopted-to-controller – Event AP adopted to wireless controller message • ap-adopted – Event access port adopted message • ap-autoup-done – Event AP autoup done message • ap-autoup-fail – Event AP autoup fail message • ap-autoup-needed – Event AP autoup needed message • ap-autoup-no-need – Event AP autoup not needed message • ap-autoup-reboot – Event AP autoup reboot message • ap-autoup-timeout – Event AP autoup timeout message • ap-autoup-ver – Event AP autoup version message • ap-reset-detected – Event access port reset detected message • ap-reset-request – Event access port user requested reset message • ap-timeout – Event access port timed out message • ap-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 • reset – Event reset message • sw-conn-lost – Event software connection lost message • unadopted – Event unadopted message
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 • client-removed – Event client removed 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

<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 • 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 • 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 • 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
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 EAP cached keys message Contd...

<event-type>	<event-name>
	• 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 • kerberos-client-failed – Event Kerberos client failed message • kerberos-client-success – Event Kerberos client success message • kerberos-wlan-failed – Event Kerberos WLAN failed message • kerberos-wlan-success – Event Kerberos WLAN success message • kerberos-wlan-timeout – Event Kerberos WLAN timeout message • move-operation-success – Event move operation success message • neighbor-denied-assoc – Event neighbor denied association message • tkip-cntrmeas-end – Event TKIP cntrmeas end message • tkip-cntrmeas-start – Event TKIP cntrmeas start message • tkip-mic-fail-report – Event TKIP mic fail report message • tkip-mic-failure – Event TKIP mic failure message • unsanctioned-ap-active – Event unsanctioned AP active message • unsanctioned-ap-inactive – Event unsanctioned AP inactive message • unsanctioned-ap-status-change – Event unsanctioned AP status change • voice-call-completed – Event voice call completed 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 related event messages • fwuaborted – Event fwu aborted message • fwubadconfig – Event fwu bad config message • fwucorruptedfile – Event fwu corrupted file message • fwucouldntgetfile – Event fwu could not get file message • fwudone – Event fwu done message • fwufileundef – Event fwu file undefined message • fwunoneed – Event fwu no need message • fwuprodmismatch – Event fwu prod mismatch message • fwuserverundef – Event fwu server undefined message • fwuserverunreachable – Event fwu server unreachable message • fwusignmismatch – Event fwu signature mismatch message • fwusyserr – Event fwu system error message • fwuunsupportedhw – Event fwu unsupported hardware message • fwuvermismatch – Event fwu 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 crit 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
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-up – Event meshpoint up message
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

<event-type>	<event-name>
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-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
securitymgr	Configures the security manager module related event messages • deprecatedcli – Event deprecated CLI message • fatal-hit – Event fatal hit message • log-cli-error – Event log CLI error message • userpassstrength – Event user pass strength message
smrt	Configures SMART RF module related event messages • calibration-done – Event calibration done message • calibration-started – Event calibration started 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
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

<event-type>	<event-name>
system	Configures system module related event messages • clock-reset – Event clock reset message • http – Event HTTP 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 • panic – Event panic 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
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
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 configuration

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
no <EVENT-TYPE> <EVENT-NAME> [email|forward-to-switch|snmp|syslog]
[default|on|off]
```

Parameters

```
no <EVENT-TYPE> <EVENT-NAME> [email|forward-to-switch|snmp|syslog]
[default|on|off]
```

no <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 The system stops network monitoring for the occurrence of the specified event and no notification is sent if the event occurs.

NOTE
For more information on the available event types and corresponding event names, see *event*.

Example

```
rfs7000-37FABE(config-event-system-policy-TestPolicy)#event ap adopted syslog
default
rfs7000-37FABE(config-event-system-policy-TestPolicy)#

rfs7000-37FABE(config-event-system-policy-TestPolicy)#no event ap 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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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:
  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

For more information on Firewall policy, see *Chapter 14, Firewall-Policy*.

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
inline-password-encryption
```

Parameters

None

Usage Guidelines:

When the configuration file is imported to a different device, it will first decrypt the encryption key using the default key and will decrypt the rest of the configuration using the administrator configured encryption key.

Example

```
rfs7000-37FABE(config)#password-encryption secret 2 12345678
rfs7000-37FABE(config)#

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 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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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
  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

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 24, 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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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
  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

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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
  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

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
meshpoint [<MESHPOINT-NAME>|containing <WORD>]
```

Parameters

```
meshpoint [<MESHPOINT-NAME>|containing]
```

<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

For more information on Meshpoint configuration, see *Chapter 28, 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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 28, 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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
mint-policy global-default
```

Parameters

```
mint-policy global-default
```

global-default	Uses the global default 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
  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

For more information on MiNT policy configuration, see *Chapter 15, Mint-Policy*.

nac-list

Global Configuration Commands

A *Network Access Control* (NAC) policy configures devices that can access a network based on their MAC addresses. Table 12 lists NAC list configuration mode commands.

TABLE 12 NAC-List Config Command

Command	Description	Reference
nac-list	Creates a NAC list and enters its configuration mode	*page 4-197*
nac-list-mode commands	Summarizes NAC list configuration mode commands	*page 4-198*

nac-list

For more information on MiNT policy configuration, see Chapter 15, Mint-Policy.

Configures a *Network Access Control* (NAC) list managing access to the network

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

For more information on MiNT policy configuration, see Chapter 15, Mint-Policy.

Table 13 summarizes NAC list configuration mode commands.

TABLE 13 NAC-List-Mode Commands

Command	Description	Reference
exclude	Specifies the MAC addresses excluded from the NAC enforcement list	*page 4-198*
include	Specifies the MAC addresses included in the NAC enforcement list	*page 4-199*
no	Cancels an exclude or include NAC list rule	*page 4-199*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
do	Runs commands from the EXEC mode	*page 4-165*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes information to memory or terminal	*page 5-310*

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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. 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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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. 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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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. 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 71XX Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
no [aaa-policy|aaa-tacacs-policy|advanced-wips-policy|br300|br650|
          br6511|br71xx|association-acl-policy|

auto-provisioning-policy|captive-portal|customize|device|device-categorizatio
n|

dhcp-server-policy|dns-whitelist|event-system-policy|firewall-policy|

igmp-snoop-policy|inline-password-encryption|ip|l2tpv3|mac|management-policy|
          meshpoint|meshpoint-qos-policy|
nac-list|password-encryption|profile|
          radio-qos-policy|radius-group|
radius-server-policy|radius-user-pool-policy|
          rf-domain|rfs4000|rfs6000|rfs7000|
role-policy|routing-policy|smart-rf-policy|
          wips-policy|wlan|wlan-qos-policy|  service]

no
[aaa-policy|aaa-tacacs-policy|advanced-wips-policy|auto-provisioning-policy|
          captive-portal|device-categorization|
dhcp-server-policy|dns-whitelist|
          event-system-policy|firewall-policy|
inline-password-encryption|ip|l2tpv3|mac|
          management-policy|meshpoint|
meshpoint-qos-policy|nac-list|radio-qos-policy|
          radius-group| radius-server-policy|
radius-user-pool-policy|role-policy|
          routing-policy|smart-rf-policy|wips-policy|wlan-qos-policy]

no [br300|br650|br6511|br71xx|rfs4000|rfs6000|rfs7000]

no device {containing <WORD>} {(filter type [br650|br6511|br71xx])}

no customize
[hostname-column-width|show-wireless-client|show-wireless-client-stats|

show-wireless-radio|show-wireless-radio-stats|show-wireless-radio-stats-rf]

no password-encryption secret 2 <OLD-PASSPHRASE>

no profile {br650|br6511|br71xx|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-system-policy|firewall-policy|
inline-password-encryption|ip|l2tpv3|mac|management-policy|
```

	`meshpoint|meshpoint-qos-policy|nac-list|radio-qos-policy|radius-group| radius-server-policy|radius-user-pool-policy|role-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 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 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 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 [br300|br650|br6511|br71xx|rfs4000|rfs6000|rfs7000] <MAC>
```

no br300	Removes an Brocade Mobility 300 Access Point from the network
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 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 device {containing <WORD>} {(filter type [br650|br6511|
br71xx|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 • 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-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|br71xx|containing|
filter} <PROFILE-NAME>
```

no profile	Removes a profile and its associated configurations
br650	Optional. Removes an Brocade Mobility 650 Access Point profile
br6511	Optional. Removes an Brocade Mobility 6511 Access Point profile

br71xx	Optional. Removes an 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 or wireless controller

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
  br300                       Delete an BRbr300300
  br650                       Delete an BR650 access point
  br6511                      Delete an BR6511 access point
  br71xx                      Delete an BR71XX access point
  association-acl-policy      Delete an association-acl policy
  auto-provisioning-policy    Delete an auto-provisioning policy
  captive-portal              Delete a captive portal
  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
```

```
  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 RFS4000 wireless controller
  rfs6000                      Delete an RFS6000 wireless controller
  rfs7000                      Delete an RFS7000 wireless controller
  role-policy                  Role based firewall policy
  routing-policy               Policy Based Routing Configuratino
  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)#
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 symbol
rfs7000-37FABE(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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
profile {br650|br6511|br71xx|containing|
          filter|rfs4000|rfs6000|rfs7000}

profile {br650|br6511|br71xx|rfs4000|rfs6000|
          rfs7000} <DEVICE-PROFILE-NAME>

profile {containing <DEVICE-PROFILE-NAME>} {filter type [br650|br6511
          |br71xx|rfs4000|rfs6000|rfs7000]}

profile {filter type [br650|br6511|br71xx|
          rfs4000|rfs6000|rfs7000]}
```

Parameters

```
profile {br650|br6511|br71xx|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
br71xx	Optional. Configures Brocade Mobility 71XX 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|br71xx|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

br71xx	Optional. Selects an Brocade Mobility 71XX 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|br71xx|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
br71xx	Optional. Selects an Brocade Mobility 71XX 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:
  ap-upgrade                      AP firmware upgrade
  br300                           Adopt/unadopt BRbr300300 device to this
                                  profile/device
  arp                             Address Resolution Protocol (ARP)
  auto-learn-staging-config       Enable learning network configuration of
                                  the devices that come for adoption
  autoinstall                     Autoinstall settings
  bridge                          Ethernet bridge
  cdp                             Cisco Discovery Protocol
  cluster                         Cluster configuration
  configuration-persistence       Enable persistence of configuration
                                  across reloads (startup config file)
  controller                      Add controller
  critical-resource               Critical Resource
  crypto                          Encryption related commands
  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
  events                          System event messages
  export                          Export a file
  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
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
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

rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands: For more information on profiles and how to configure profiles, see *Chapter 7, Profiles*.

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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)#
```

Related Commands: For more information on radio qos policy, see *Chapter 18, Radio-QOS-Policy*.

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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)#
```

Related Commands: For more information on RADIUS user group commands, see *Chapter 17, Radius-Policy*.

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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)#
```

Related Commands: For more information on RADIUS server policy commands, see *Chapter 17, Radius-Policy*.

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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)#
```

Related Commands: For more information on RADIUS user group commands, see *Chapter 17, Radius-Policy*.

no	Removes an existing RADIUS user pool

rf-domain

Global Configuration Commands

An RF Domain groups devices that can logically belong to one network. Table 14 lists the RF Domain configuration mode commands.

TABLE 14 RF-Domain Config Commands

Command	Description	Reference
rf-domain	Creates a RF Domain policy and enters its configuration mode	*page 4-212*
rf-domain-mode commands	Invokes RF Domain configuration mode commands	*page 4-214*

rf-domain

rf-domain

Creates an RF Domain or enters the RF Domain configuration context for one or more RF Domains. If the policy does not exist, it creates a new policy.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 the RF Domain configuration context for one or more existing RF Domains
<RF-DOMAIN-NAME>	Optional. Specify the RF Domain name. The name should not exceed 32 characters and should represent the intended purpose. Once created, the name cannot be edited.
containing <DOMAIN-NAME>	Optional. Specify 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:
  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
  country-code      Configure the country of operation
  dhcp-redundancy   Enable DHCP redundancy
  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
  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.

Table 15 summarises RF Domain configuration commands.

TABLE 15 RF-Domain-Mode Commands

Command	Description	Reference
channel-list	Configures the channel list advertised by radios	*page 4-214*
contact	Configures network administrator's contact information (needed in case of any problems impacting the RF Domain)	*page 4-215*
control-vlan	Configures VLAN for traffic control on a RF Domain	*page 4-216*
country-code	Configures the country of operation	*page 4-217*
dhcp-redundancy	Enables DHCP redundancy on a RF Domain	*page 4-217*
layout	Configures layout information	*page 4-218*
location	Configures the physical location of a RF Domain	*page 4-219*
mac-name	Maps MAC addresses to names	*page 4-220*
no	Negates a command or reverts configured settings to their default	*page 4-221*
override-smart-rf	Configures RF Domain level overrides for Smart RF	*page 4-223*
override-wlan	Configures RF Domain level overrides for a WLAN	*page 4-223*
sensor-server	Configures an AirDefense sensor server on this RF Domain	*page 4-224*
stats	Configures stats related settings on this RF Domain. These settings define how RF Domain statistics are updated	*page 4-225*
timezone	Configures a RF Domain's geographic time zone	*page 4-226*
use	Enables the use of a specified Smart RF and/or WIPS policy	*page 4-227*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
do	Runs commands from the EXEC mode	*page 4-165*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes information to memory or terminal	*page 5-310*

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
control-vlan <1-4094>
```

Parameters

```
control-vlan <1-4094>
```

<1-4094>	Specify the VLAN ID from 1 - 4094.

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

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

dhcp-redundancy

rf-domain-mode commands

Enables DHCP redundancy in this RF Domain

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
dhcp-redundancy
```

Parameters

None

Example

```
rfs7000-37FABE(config-rf-domain-default)#dhcp-redundancy

rfs7000-37FABE(config-rf-domain-default)#show context
rf-domain default
 contact Bob+919621212577
 country-code in
 dhcp-redundancy
 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 RF Domain DHCP redundancy

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
layout [area|floor|map-location]

layout [(area <AREA-NAME>|floor <FLOOR-NAME>)]

layout map-location <URL> units [feet|meters] {(area <AREA-NAME>|floor
<FLOOR-NAME>)}
```

Parameters

```
layout [(area <AREA-NAME>|floor <FLOOR-NAME>)]
```

layout	Configures the RF Domain layout in terms of area, floor, and location on a map
area <AREA-NAME>	Configures the RF Domain area name • <AREA-NAME> – Specify the area name.
floor <FLOOR-NAME>	Configures the RF Domain floor name • <FLOOR-NAME> – Specify the floor name.

```
layout map-location <URL> units [feet|meters] {(area <AREA-NAME>|
floor <FLOOR-NAME>)}
```

layout	Configures the RF Domain layout in terms of area, floor, and location on a 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. • units [feet|meters] – Configures the map units in terms of feet or meters After configuring the location, optionally configure the area and floor of the RF Domain.
area <AREA-NAME>	Optional. Configures the RF Domain area name. Specify area name.
floor <FLOOR-NAME>	Optional. Configures the RF Domain floor name. Specify floor 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
 dhcp-redundancy
 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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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
 dhcp-redundancy
 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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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
 dhcp-redundancy
 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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
no
[channel-list|contact|control-vlan|country-code|dhcp-redundancy|layout|locati
on|

mac-name|override-smartrf|override-wlan|sensor-server|stats|timezone|use]
```

Parameters

```
no [channel-list|contact|control-vlan|country-code|dhcp-redundancy|layout|
location|
mac-name|override-smartrf|override-wlan|sensor-server|stats|timezone|use]
```

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 country-code	Removes the country of operation configured
no dhcp-redundancy	Removes DHCP redundancy
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 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
 dhcp-redundancy
 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:

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
country-code	Configures a RF Domain’s country of operation
dhcp-redundancy	Enables a RF Domain’s DHCP redundancy
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
use	Enables the use of a Smart RF and/or WIPS policy

override-smart-rf

rf-domain-mode commands

Configures RF Domain level overrides for a Smart RF policy

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
override-smartrf channel-list [2.4GHz|5GHZ] <CHANNEL-LIST>
```

Parameters

```
override-smartrf channel-list [2.4GHz|5GHZ] <CHANNEL-LIST>
```

override-smartrf	Configures RF Domain level overrides for a Smart RF policy
channel-list	Enables the selection of a channel list for a Smart RF policy
2.4GHz <CHANNEL-LIST>	Selects the 2.4 GHz band • <CHANNEL-LIST> – Specify a list of channels separated by commas.
5GHz <CHANNEL-LIST>	Selects the 5.0 GHz band • <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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 *Service Set Identifier* (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.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

use

rf-domain-mode commands

Enables the use of Smart RF and WIPS with this RF Domain

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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.
wips-policy <WIPS-POLICY-NAME>	Specifies a WIPS policy <WIPS-POLICY-NAME> – Specify the WIPS policy name.

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

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

Syntax:

```
rfs4000 <DEVICE-Brocade Mobility RFS4000>
```

Parameters

```
rfs4000 <DEVICE-Brocade Mobility RFS4000>
```

<DEVICE-Brocade Mobility RFS4000>	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

Syntax:

```
rfs6000 <DEVICE-Brocade Mobility RFS6000>
```

Parameters

```
rfs6000 <DEVICE-Brocade Mobility RFS6000>
```

<DEVICE-Brocade Mobility RFS6000>	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

Syntax:

```
rfs7000 <DEVICE-Brocade Mobility RFS7000>
```

Parameters

```
rfs7000 <DEVICE-Brocade Mobility RFS7000>
```

<DEVICE-Brocade Mobility RFS7000>	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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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-mode        Change the ldap mode
  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)#
```

Related Commands: For more information on role policy commands, see *Chapter 19, Role-Policy*.

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 26, 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 71XX Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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
  root-recovery           Recover issues due to poor root path metric
  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)#
```

Related Commands: For more information on Smart RF policy commands, see *Chapter 20, Smart-RF-Policy*.

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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:
  ap-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)#
```

Related Commands: For more information on WIPS policy commands, see *Chapter 21, WIPS-Policy*.

no	Removes an existing WIPS policy

wlan

Global Configuration Commands

Configures a wireless LAN. Table 16 lists WLAN configuration mode commands.

TABLE 16 WLAN-Policy Config Commands

Command	Description	Reference
wlan	Creates a new wireless LAN and enters its configuration mode	*page 4-234*
wlan-mode commands	Summarizes WLAN configuration mode commands	*page 4-236*

wlan

wlan

Configures a WLAN or enters the WLAN configuration context for one or more WLANs

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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.
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.

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
  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
  data-rates                   Specify the 802.11 rates to be supported on
                               this wlan
  description                  Configure a description of the usage of this
                               wlan
  encryption-type              Configure the encryption to use on this wlan
  enforce-dhcp                 Drop packets from Wireless Clients with static
                               IP address
  http-analyze                 Enable HTTP URL analysis on the wlan
  ip                           Internet Protocol (IP)
  kerberos                     Configure kerberos authentication 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
  radius                       Configure RADIUS related parameters
  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

Configures WLAN mode commands. Manual WLAN mappings are erased when the actual WLAN is disabled and then enabled immediately.

Use the (config) instance to configure WLAN related parameters.

To navigate to this instance, use the following commands:

```
rfs7000-37FABE(config)#wlan <WLAN-NAME>
```

Table 17 summarizes WLAN configuration mode commands.

TABLE 17 WLAN-Mode Commands

Command	Description	Reference
accounting	Defines a WLAN accounting configuration	*page 4-237*
acl	Defines the actions based on an ACL rule configuration	*page 4-238*
answer-broadcast-probes	Allows a WLAN to respond to probes for broadcast ESS	*page 4-239*
authentication-type	Sets a WLAN's authentication type	*page 4-240*
bridging-mode	Configures how packets to/from this WLAN are bridged	*page 4-241*
broadcast-dhcp	Configures broadcast DHCP packet handling	*page 4-241*
broadcast-ssid	Advertises a WLAN's SSID in beacons	*page 4-242*
captive-portal-enforcement	Configures a WLAN's captive portal enforcement	*page 4-242*
client-access	Enables WLAN client access (normal data operations)	*page 4-243*
client-client-communication	Allows the switching of frames from one wireless client to another on a WLAN	*page 4-243*
client-load-balancing	Enables load balancing of WLAN clients	*page 4-244*
data-rates	Specifies the 802.11 rates supported on the WLAN	*page 4-245*
description	Sets a WLAN's description	*page 4-247*
encryption-type	Sets a WLAN's encryption type	*page 4-248*
enforce-dhcp	Drops packets from clients with a static IP address	*page 4-249*
http-analyze	Enables HTTP URL analysis on the WLAN	*page 4-250*
ip	Configures IP settings	*page 4-251*

TABLE 17 WLAN-Mode Commands

Command	Description	Reference
kerberos	Configures Kerberos authentication parameters	*page 4-252*
mac-registration	Enables dynamic MAC registration of user	*page 4-254*
motorola-extensions	Enables support for Brocade specific extensions to 802.11	*page 4-255*
no	Negates a command or reverts settings to their default	*page 4-256*
proxy-arp-mode	Enables the proxy ARP mode for ARP requests	*page 4-258*
radius	Configures RADIUS parameters	*page 4-259*
shutdown	Closes a WLAN	*page 4-260*
ssid	Configures a WLAN's SSID	*page 4-261*
time-based-access	Configures time-based client access	*page 4-261*
use	Defines WLAN mode configuration settings	*page 4-262*
vlan	Sets VLAN assignment for a WLAN	*page 4-264*
vlan-pool-member	Adds a member VLAN to the pool of VLANs for a WLAN	*page 4-265*
wep128	Configures WEP128 parameters	*page 4-266*
wep64	Configures WEP64 parameters	*page 4-267*
wireless-client	Configures the transmit power for wireless clients transmission	*page 4-269*
wpa-wpa2	Modifies TKIP and CCMP (WPA/WPA2) related parameters	*page 4-271*

accounting

wlan-mode commands

Defines the WLAN's accounting configuration

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
accounting [radius|syslog]

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
```

accounting radius	Enables support for WLAN RADIUS accounting messages

	`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
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 – Requests are proxied through the wireless controller configuring the device • through-rf-domain-manager – Requests are proxied 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

Supported in the following platforms:

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

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 an SSID. These probes are for broadcast ESS.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
answer-broadcast-probes
```

Parameters

None

Example

```
rfs7000-37FABE(config-wlan-1)#answer-broadcast-probes
rfs7000-37FABE(config-wlan-1)#
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 *Extensible Authentication Protocol* (EAP) authentication (802.1X)
eap-mac	Configures EAP or MAC authentication depending on client
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)).
kerberos	Configures Kerberos authentication (encryption will change to WEP128 if it's not already WEP128 or Keyguard)
mac	Configures MAC authentication (RADIUS lookup of MAC address)
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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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). 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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

Supported in the following platforms:

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

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 time 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)#
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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-mcs0-7|mcs0-15|mcs0-7|mcs8-15]

data-rates 5GHz [a-only|an|custom|default]
```

```
data-rates 5GHz custom [12|18|24|36|48|54|6|9|basic-1|basi-11|

basic-12|basic-18|basic-2|basic-24|basic-36|basic-48|basic-5.5|basic-54|
          basic-6|basic-9|basic-mcs0-7|mcs0-15|mcs0-7|mcs8-15]
```

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-mcs0-7|mcs0-15|mcs0-7|mcs8-15]
```

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-mcs0-7,mcs0-15, mcs0-7,mcs8-15	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-mcs0-7 – Modulation and coding scheme 0-7 as a basic rate • mcs0-15 – Modulation and coding scheme 0-15 • mcs0-7 – Modulation and coding scheme 0-7 • mcs8-15 – Modulation and coding scheme 8-15

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
description <LINE>
```

Parameters

```
description <LINE>
```

<LINE>	Specify a WLAN description

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)#
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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)#
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
http-analyze [controller|filter|syslog]

http-analyze filter [images|strip-query-string]

http-analyze syslog host <IP/HOSTNAME> {port <1-65535>} {proxy-mode [none|
          through-controller|through-rf-domain-manager]}
```

Parameters

`http-analyze controller`

controller	Forwards client and URL information to the wireless controller through the adopted AP

`http-analyze filter [images|strip-query-string]`

filter	Filters URLs, based on the parameters set, before forwarding them
images	Filters out URLs referring to images
strip-query-string	Strips query strings from URLs before forwarding them

`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 through the wireless controller configuring the device • through-rf-domain-manager – Proxies the requests through the local RF Domain manager

Example

```
rfs7000-37FABE(config-wlan-test)#http-analyze controller

rfs7000-37FABE(config-wlan-test)#show context
wlan test
 description TestWLAN
 ssid test
 bridging-mode local
 encryption-type tkip-ccmp
 ..................................................
 captive-portal-enforcement fall-back
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 enforce-dhcp
 broadcast-dhcp validate-offer
 http-analyze controller
rfs7000-37FABE(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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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-registration

wlan-mode commands

Enables dynamic MAC registration of a user

Supported in the following platforms:This feature is supported only if MAC authentication is enabled. To enable MAC authentication use the *authentication-type* > *mac* command in the WLAN config mode.

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
mac-registration [external|group-name]

mac-registration external host <IP/HOSYTNAME> {proxy-mode
[none|through-controller|
          through-rf-domain-manager]}
mac-registration group-name <GROUP-NAME> {expiry-time <1-1500>}
```

Parameters

```
mac-registration external host <IP/HOSYTNAME> {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 external wireless controller
host <IP/HOSTNAME>	Specifies the external wireless 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 wireless controller from requesting device • through-controller – Requests are proxied through the wireless controller configuring the device • through-rf-domain – Requests are proxied through the local RF Domain Manager

```
mac-registration group-name <GROUP-NAME> {expiry-time <1-1500>}]
```

mac-registration	Enables dynamic MAC registration of 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 - 15000

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)#
```

motorola-extensions

wlan-mode commands

Enables support for Brocade specific extensions to 802.11

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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
  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
  data-rates                   Reset data rate configuration to default
  description                  Reset the description of the 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
  http-analyze                 Enable HTTP URL analysis on the wlan
  ip                           Internet Protocol (IP)
```

```
  kerberos                    Configure kerberos authentication 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
  radius                      Configure RADIUS related parameters
  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 Commands

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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)#
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

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)#
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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
on-critical-resource	Optional. Shuts down the WLAN when critical resource failure occurs
on-meshpoint-loss	Optional. Shuts down the WLAN when the root meshpoint link fails (is unreachable)
on-primary-port-link-loss	Optional. Shuts down the WLAN when a device losses its primary Ethernet port (ge1/up1) link
on-unadoption	Optional. Shuts down the WLAN when an adopted device becomes unadopted

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
ssid <SSID>
```

Parameters

```
ssid <SSID>
```

<SSID>	Specify the WLAN's SSID. The WLAN SSID is case sensitive and alphanumeric. It's 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 client access to network resources based on the defined time

Supported in the following platforms:

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

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
time-based-access day [sunday|monday|tuesday|wednesday|thursday|friday|
          saturday|all|weekends|weekdays] {start <START-TIME>} [end
<END-TIME>]
```

Parameters

```
time-based-access day [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 • Tuesdays – 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)

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
 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)#
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
use [aaa-policy|association-acl-policy|captive-portal|ip-access-list|
          mac-access-list|wlan-qos-policy]

use [aaa-policy <AAA-POLICY-NAME>|association-acl-policy <ASSOCIATION-POLICY-
NAME>|
          captive-portal <CAPTIVE-PORTAL-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>|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.
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.

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
vlan <1-4094>
```

Parameters

```
vlan <1-4094>
```

<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.

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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>	Defines the VLAN configuration. 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
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 use aaa-policy test
 use association-acl-policy test
--More--
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 • <1-4> – Specify a key index from 1 - 4.

Example

```
rfs7000-37FABE(config-wlan-test)#wep128 keys-from-passkey exampleutions@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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 • <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--
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
wireless-client
[count-per-radio|cred-cache-ageout|hold-time|inactivity-timeout|

max-firewall-sessions|reauthentication|roam-notification|tx-power|vlan-cache-
out]

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 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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 msec - 5000 msec. • <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--
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 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)#
```

Related Commands: For more information on WLAN QoS policy commands, see *Chapter 22, WLAN-QOS-Policy*.

no	Removes an existing WLAN QoS Policy

Chapter

Common Commands 5

In this chapter

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 18 summarizes commands common to the User Exec, Priv Exec, and Global Config modes.

TABLE 18 Commands Common to Wireless Controller CLI Modes

Command	Description	Reference
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
exit	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
no	Negates a command or reverts values to their default settings	*page 5-281*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 5-283*
show	Displays running system information	*page 5-309*
write	Writes the system's running configuration to memory or terminal	*page 5-310*

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
clrscr
```

Parameters

None

Example

```
The terminal window or screen before the clrscr command is executed:
rfs7000-37FABE#ap-upgrade ?
  DEVICE-NAME     Name/MAC address of AP
  all             Upgrade all access points
  br650           Upgrade an BR650 device
  br6511          Upgrade an BR6511 device
  br71xx          Upgrade an BR71XX device
  cancel-upgrade  Cancel upgrading the AP
  load-image      Load the AP images to controller for ap-upgrades
  rf-domain       Upgrade all access points belonging to an RF Domain

rfs7000-37FABE#

The terminal window or screen after the clrscr command is executed:
rfs7000-37FABE#
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 specific target term • <WORD> – Specify a target term (for example, a feature, or 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-ap-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|BR
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:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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
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
  br300                     Delete an br300
```

```
  br650                       Delete an BR650 access point
  br6511                      Delete an BR6511 access point
  br71xx                      Delete an BR71XX access point
  association-acl-policy      Delete an association-acl policy
  auto-provisioning-policy    Delete an auto-provisioning policy
  captive-portal              Delete a captive portal
  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
  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 RFS4000 wireless controller
  rfs6000                     Delete an RFS6000 wireless controller
  rfs7000                     Delete an RFS7000 wireless controller
  role-policy                 Role based firewall policy
  routing-policy              Policy Based Routing Configuratino
  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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
revert
```

Parameters

None

Example

```
rfs7000-37FABE>revert
rfs7000-37FABE>
```

service

Common Commands

5

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 of the current mode's CLI tree.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax: (User Exec Mode)

```
service [advanced-wips|br300|clear|cli-tables-expand|cli-tables-skin|cluster|

delete-offline-aps|disable|enable|force-send-config|load-balancing|locator|
          radio|radius|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-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-ap-detection|
          stp-detection|unauthorized-bridge|windows-zero-config-memory-leak|
          wlan-jack-attack-detected}

service br300 [dns-name|dot1x|locator|reload]
service br300 dns-name <DNS-NAME> on [all|ap-mac <MAC>]
service br300 dot1x username <USERNAME> password <PASSWORD> on [all|ap-mac
<MAC>]
service br300 [locator|reload] <MAC>

service clear [ap-upgrade|captive-portal-page-upload|command-history|noc|
          reboot-history|unsanctioned|upgrade-history|wireless|xpath]
service clear ap-ugrade history {on <DOMAIN-NAME>}
service clear captive-portal-page-upload history {on <DOMAIN-NAME>}
service clear [command-history|reboot-history|upgrade-history] {on
<DEVICE-NAME>}
service clear noc statistics
service clear unsanctioned aps {on <DEVICE-OR-DOMAIN-NAME>}
service clear wireless [ap|client|radio|wlan]
```

```
service clear wireless [ap|client] statistics {<MAC>} {(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-expand {left|right}

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 radiusd

service force-send-config {on <DEVICE-OR-DOMAIN-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> ssid <SSID>} {(on <DEVICE-NAME>)}

service set validation-mode [full|partial] {on <DEVICE-NAME>}

service show [advanced-wips|captive-portal|cli|command-history|
configuration-revision|
          crash-info|dhcp-lease|diag|fib|info|mac-vendor|mem|
mint|noc|pm|process|
          reboot-history|rf-domain-manager|snmp|startup-log|sysinfo|
top|upgrade-history|
          watch-dog|wireless|xpath-history]

service show advanced-wips stats
[ap-table|client-table|connected-sensors-status|
          termination-entries]
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>|on|ppppoe1|vlan <1-4094>|wwan1}
          {(on <DEVICE-NAME>)}
service show diag [led-status|stats] {on <DEVICE-NAME>}
```

```
service show fib {table-id <0-255>}
service show mint adopted-devices {on <DEVICE-NAME>}
service show pm {history} {(on <DEVICE-NAME>)}
service show rf-domain-manager diag {<MAC/HOSTNAME>} {(on <DEVICE-OR-DOMAIN-
NAME>)}

service show wireless
[aaa-stats|br300|client|config-internal|credential-cache|
          dns-cache|log-interval|meshpoint|neighbors|reference|stats-client|
vlan-usage]
service show wireless [aaa-stats|credential-cache|dns-cache|vlan-usage] {on
<DEVICE-NAME>}
service show wireless [br300 <MAC>|config-internal|log-interval|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|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

service wireless [client|dump-core-snapshot|meshpoint|qos|wips]

service wireless client [beacon-request|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 trigger-bss-transition <MAC> url <URL> {on
<DEVICE-OR-DOMAIN-
          NAME>}
service wireless meshpoint zl <MESHPOINT-NAME> [on <DEVICE-NAME>] {<ARGS>}
service wireless qos delete-tspec <MAC> tid <0-7>
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 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-detection*| *multicast-rip2-routers-detection*|*multicast-vrrp-agent*|*netbios-detection*| *null-probe-response-detected*|*probe-response-flood*|*rogue-ap-detection*| *stp-detection*| *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-ap-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 or wireless client.

`service br300 dns-name <DNS-NAME> on [all|ap-mac <MAC>]`

br300	Sets global br300 configuration parameters
dns-name <DNS-NAME>	Authenticates DNS server name for AP adoption • <DNS-NAME> – Specify the DNS sever name.
on [all|ap-mac <MAC>]	Adopts a specified br300 or all BR300s • all – Adopts all BR300s • ap-mac <MAC> – Adopts a specified BR300 • <MAC> – Specify the Brocade Mobility 300 Access Point's MAC address.

`service br300 dot1x username <USERNAME> password <PASSWORD> on [all|ap-mac <MAC>]`

br300	Configures global BR300 parameters
dot1x	Sets 802.1x authentication parameters
username <USERNAME>	Authenticates user before providing access • <USERNAME> – Specify the username to authenticate.
password <PASSWORD>	Authenticates password before providing access • <PASSWORD> – Specify the password.
on [all|ap-mac <MAC>]	Configures global BR300 parameters on a specified BR300 or all BR300s • all – Sets global parameters on all BR300s • BR300 <MAC> – Configures global parameters on a specified BR300 • <MAC> – Specify the Brocade Mobility 300 Access Point's MAC address.

	`service br300 [locator|reload] <MAC>`
br300	Configures global BR300 parameters
locator	Enables a specified BR300's LEDs
reload	Resets a specified BR300
<MAC>	The following keyword is common to 'locator' and 'reload' parameters: Specifies the Brocade Mobility 300 Access Point's MAC address to enable its locator or to reset the device • <MAC> – Specify the Brocade Mobility 300 Access Point's MAC address.

	`service clear ap-upgrade history` *{on <DOMAIN-NAME>}*
clear ap-upgrade history	Clears AP firmware upgrade history
on <DOMAIN-NAME>	Optional. Clears AP firmware upgrade history on 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]` *{on <DEVICE-NAME>}*
clear [command-history| reboot-history| upgrade-history]	Clears command history, reboot history, or device upgrade history
on <DEVICE-NAME>	Optional. Clears history on a specified device • <DEVICE-NAME> – Specify the name of the AP or wireless controller.

	`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, or RF Domain.

	`service clear wireless [ap|client]` *{<MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}*
clear wireless [ap|client] statistics	Clears wireless statistics counters based on the parameters passed • ap 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 'ap' 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, or RF Domain.

	`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, 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, 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. Omits for this session
	`service cli-tables-expand {left|right}`
cli-tables-expand	Displays the CLI table in a drop-down format
left	Optional. Displays the output in a left-justified format
right	Optional. Displays the output in a right-justified format
	`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 radiusd`

enable radius	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> – Optional. Specify the name of the AP, wireless controller, or RF Domain.

`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 or wireless controller.

`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 or wireless controller.

`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 • test – Tests RADIUS server account with user 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 or wireless controller.

	`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 account • test – Tests the RADIUS server account with user 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 or wireless controller.

	`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 or wireless controller.

	`service show advanced-wips stats [ap-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
ap-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 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 or wireless controller.

	`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-histroy| 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 or wireless controller.

`service show dhcp-lease {<INTERFACE-NAME>|on|ppppoe1|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
ppppoe1	Optional. Displays DHCP lease information for a PPP over Ethernet interface
vlan <1-4094>	Optional. Displays DHCP lease information for a VLAN • <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 or wireless controller.

`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 or wireless controller.

`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>)}`

show	Displays running system statistics based on the parameters passed
mint	Displays MiNT protocol details

adopted-devices	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 or wireless controller.

`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 or wireless controller.

`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, or RF Domain.

`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 or wireless controller.

`service show wireless [br300 <MAC>|config-internal|log-interval|neighbors]`

show	Displays running system statistics based on the parameters passed
wireless	Displays WLAN statistics (WLAN AAA policy, configuration parameters, VLAN usage etc.)
br300 <MAC>	Displays a WLAN's BR300 statistics • <MAC> – Specify the MAC address of the BR300.
config-internal	Displays internal configuration parameters
log-interval	Displays recent wireless debug logs (info and above severity)
neighbors	Displays neighboring device statistics for roaming and flow migration

	`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 These proc entries provide statistics on each wireless client on the WLAN. 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, or RF Domain.

```
service smart-rf [clear-config|clear-history|interactive-calibration|
run-calibration|save-config|stop-calibration] {on <DOMAIN-NAME>}
```

smart-rf	Enables Smart RF management
clear-config	Clears a WLAN Smart RF configuration on all devices
clear-history	Clears a 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 Domain Manager
stop-calibration	Stops an in-progress Smart RF configuration
on <DOMAIN-NAME>	Optional. Enables Smart RF management on 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 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 MAC address of the wireless client.
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 or wireless controller.

`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, or RF Domain.

`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-NAME> meshpoint
on <DEVICE-NAME>	Runs zonal commands for a specified meshpoint on a specified AP or wireless controller
<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 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 MAC address of the wireless client.

`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, 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
[advanced-wips|br300|clear|cli-tables-expand|cli-tables-skin|cluster|copy|

delete|delete-offline-aps|force-send-config|load-balancing|locator|mint|pktca
p|
          pm|radio|
radius|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 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 in the following format: cf:/path/file usb1:/path/file usb2:/path/file
<URL>	Specify the 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

`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 or wireless controller.

`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 or wireless controller.

	`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|priorit y|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 Contd..

	• 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 – Match 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: (Global Config Mode)

```
service [set|show cli]
service set [command-history <10-300>|upgrade-history <10-100>|
          reboot-history <10-100>] {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.
on <DEVICE-NAME>	Optional. Sets the size of history files on a specified device • <DEVICE-NAME> – Specify the name of the AP or wireless controller.

`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)#

rfs7000-37FABE>service show command-history on rfs7000-37FABE
Configured size of command history is 200

  Date & Time          User      Location           Command
=====================================================================
May 10 08:53:38 2012   admin     172.16.10.12 16      exit
May 10 08:18:50 2012   admin     172.16.10.12 15      exit
May 10 07:38:23 2012   admin     172.16.10.12 14      service advanced-wips
clear-event-history
May 10 07:35:17 2012   admin     172.16.10.12 13      exit
May 10 07:32:34 2012   admin     172.16.10.12 13      exit
May 10 07:28:00 2012   admin     172.16.10.12 10      exit
May 09 14:45:09 2012   admin     172.16.10.10 52      reload force
May 09 14:45:08 2012   admin     172.16.10.10 52      write memory
May 09 13:25:40 2012   admin     172.16.10.12 49      exit
May 09 13:25:39 2012   admin     172.16.10.12 49      revert
May 09 13:23:22 2012   admin     172.16.10.12 49      exit
May 09 12:56:46 2012   admin     172.16.10.12 49      no mark-device 1
sanctioned ap mac 11-22-33-44-55-66
May 09 12:56:29 2012   admin     172.16.10.12 49      exit
May 09 12:55:19 2012   admin     172.16.10.12 49      mark-device 1 sanctioned
ap mac
11-22-33-44-55-66
May 09 12:54:47 2012   admin     172.16.10.12 49      no mark-device 2
May 09 12:54:05 2012   admin     172.16.10.12 49     mark-device 2 neighboring
--More--
rfs7000-37FABE>

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>service show info on rrfs7000-37FABE
7.7M out of 8.0M available for logs.
9.4M out of 10.0M available for history.
19.2M out of 20.0M available for crashinfo.

List of Files:

cfgd.log                                5.7K    Jul 28 17:17
fmgr.log                                221     Jul 27 12:40
messages.log                            1.0K    Jul 27 12:41
startup.log                             52.3K   Jul 27 12:40
command.history                         903     Jul 28 16:39
reboot.history                          1.6K    Jul 27 12:40
ugrade.history                          698     Jul 27 12:39

Please export these files or delete them for more space.

rfs7000-37FABE>

rfs7000-37FABE>service show upgrade-history on rfs7000-37FABE
Configured size of upgrade history is 50

  Date & Time            Old Version     New Version     Status
=====================================================================
Jun 07 07:25:49 2012 5.4.0.0-015D 5.4.0.0-019D Successful
May 28 09:25:26 2012 5.4.0.0-011D 5.4.0.0-015D Successful
May 15 11:18:32 2012 5.4.0.0-010D 5.4.0.0-011D Successful
May 15 11:16:33 2012 5.4.0.0-010D 5.4.0.0-010D Unable to get update file.
ftpget: unexpected server response to RETR: 550 Latestbuilds/Brocade Mobility
RFS7000.img: The system cannot find the file specified.
May 15 11:14:51 2012 5.4.0.0-010D 5.4.0.0-010D Unable to get update file.
ftpget: unexpected server response to RETR: 550 Latestbuilds/RFS70Brocade
Mobility RFS7000-5.4.0.0-011D.img: The system cannot find the file specified.
May 09 14:40:22 2012 5.4.0.0-149320X 5.4.0.0-010D Successful
Apr 27 17:04:40 2012 5.4.0.0-147995X 5.4.0.0-149320X Successful
Apr 17 16:01:37 2012 5.4.0.0-146545X 5.4.0.0-147995X Successful
Apr 05 10:06:35 2012 5.4.0.0-144745X 5.4.0.0-146545X Successful
Mar 28 15:18:48 2012 5.4.0.0-144745X 5.4.0.0-145763X Successful
Mar 19 13:45:32 2012 5.4.0.0-144571X 5.4.0.0-144745X Successful
Mar 19 11:16:31 2012 5.4.0.0-005D 5.4.0.0-144571X Successful
Mar 19 11:15:57 2012 Package SigningCerts 0.0 Successful
Mar 19 11:15:51 2012 5.4.0.0-005D 5.4.0.0-005D Unable to get update file.
ftpget: unexpected server response to RETR: 550
LatestBuilds/Patches/SigningCerts.path
--More--
rfs7000-37FABE>

rfs7000-37FABE>service show xpath-history
--------------------------------------------------------------------------------
------------------------------------------------------------
     DATE&TIME       USER                        XPATH
DURATION(MS)
--------------------------------------------------------------------------------
------------------------------------------------------------
```

```
  Thu May 10 08:59:42 2012   system
/wing-stats/device/00-15-70-37-FA-BE/upgrade-history
10
  Thu May 10 08:59:05 2012   system
/wing-stats/device/00-15-70-37-FA-BE/service-info
139
  Thu May 10 08:58:26 2012   system
/wing-stats/device/00-15-70-37-FA-BE/diag/temp
23
  Thu May 10 08:58:26 2012   system
/wing-stats/device/00-15-70-37-FA-BE/diag/fan
41
  Thu May 10 08:57:01 2012   system
/wing-stats/device/00-15-70-37-FA-BE/command-history
19
  Thu May 10 08:09:12 2012   system
/wing-stats/device/00-15-70-37-FA-BE/system
135
--------------------------------------------------------------------------------
----------
rfs7000-37FABE>

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#
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
show <PARAMETER>
```

Parameters

None

Example

```
rfs7000-37FABE#show ?
  adoption                    Display information related to adoption to
                              wireless controller
  advanced-wips               Advanced WIPS
  ap-upgrade                  AP Upgrade
  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
  dot1x                       802.1X
  event-history               Display event history
  event-system-policy         Display event system policy
  file                        Display filesystem information
  firewall                    Wireless Firewall
  interface                   Interface Configuration/Statistics commands
  ip                          Internet Protocol (IP)
  ip-access-list-stats        IP Access list stats
  l2tpv3                      L2TPv3 information
  licenses                    Show installed licenses and usage
  lldp                        Link Layer Discovery Protocol
  logging                     Show logging information
  mac-access-list-stats       MAC Access list stats
  mac-address-table           Display MAC address table
```

```
  mint                        MiNT protocol
  noc                         Noc-level information
  ntp                         Network time protocol
  password-encryption         Pasword encryption
  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
  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#
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
write [memory|terminal]
```

Parameters

```
write [memory|terminal]
```

memory	Writes to the *non-volatile* (NV) memory
terminal	Writes to terminal

Example

```
rfs7000-37FABE>write memory
[OK]
rfs7000-37FABE>
```

5

Chapter

Show Commands

6

In this chapter

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 19 summarizes show commands.

TABLE 19 Show Commands

Command	Description	Reference
show	Displays settings for the specified system component	*page 6-315*
adoption	Displays information related to adoption	*page 6-319*
advanced-wips	Displays advanced *Wireless Intrusion Prevention System* (WIPS) settings	*page 6-320*
ap-upgrade	Displays access point software image upgrade information	*page 6-322*
boot	Displays a device boot configuration	*page 6-324*
captive-portal	Displays WLAN hotspot functions	*page 6-325*
captive-portal-page-upload	Displays captive portal page related information	*page 6-327*
cdp	Displays a *Cisco Discovery Protocol* (CDP) neighbor table	*page 6-328*
clock	Displays the software system clock	*page 6-330*
cluster	Displays cluster commands	*page 6-330*
commands	Displays command list	*page 6-331*
context	Displays information about the current context	*page 6-332*
critical-resources	Displays critical resource information	*page 6-334*

TABLE 19 Show Commands

Command	Description	Reference
crypto	Displays encryption mode information	*page 6-334*
debug	Displays the Xpath module debugging information	*page 6-337*
debugging	Displays debugging information on all modules other than the Xpath module	*page 6-339*
dot1x	Displays dot1x information on interfaces	*page 6-341*
event-history	Displays event history	*page 6-342*
event-system-policy	Displays event system policy configuration information	*page 6-343*
file	Displays file system information	*page 6-344*
firewall	Displays wireless firewall information	*page 6-344*
interface	Displays interface status	*page 6-347*
ip	Displays IP related information	*page 6-349*
ip-access-list-stats	Displays IP access list statistics	*page 6-354*
l2tpv3	Displays *Layer 2 Tunnel Protocol Version 3* (L2TPV3) information	*page 6-355*
licenses	Displays installed licenses and usage information	*page 6-357*
lldp	Displays *Link Layer Discovery Protocol* (LLDP) information	*page 6-357*
logging	Displays logging information	*page 6-358*
mac-access-list-stats	Displays MAC access list statistics	*page 6-359*
mac-address-table	Displays MAC address table entries	*page 6-360*
mint	Displays MiNT protocol configuration commands	*page 6-360*
noc	Displays *Network Operations Center* (NOC) level information	*page 6-363*
ntp	Displays *Network Time Protocol* (NTP) information	*page 6-365*
password-encryption	Displays password encryption status	*page 6-366*
pppoe-client	Displays *Point to Point Protocol over Ethernet* (PPPoE) client information	*page 6-366*
privilege	Displays current privilege level information	*page 6-367*
reload	Displays scheduled reload information	*page 6-368*
remote-debug	Displays remote debug session data	*page 6-368*
rf-domain-manager	Displays RF Domain manager selection details	*page 6-369*
role	Displays role-based firewall information	*page 6-370*
route-maps	Display route map statistics	*page 6-370*
rtls	Displays *Real Time Location Service* (RTLS) statistics of access points	*page 6-371*
running-config	Displays configuration file contents	*page 6-371*
session-changes	Displays configuration changes made in this session	*page 6-375*
session-config	Displays a list of currently active open sessions on the device	*page 6-376*
sessions	Displays CLI sessions	*page 6-377*
smart-rf	Displays Smart RF management commands	*page 6-377*
spanning-tree	Displays spanning tree information	*page 6-380*
startup-config	Displays complete startup configuration script on the console	*page 6-383*

TABLE 19 Show Commands

Command	Description	Reference
terminal	Displays terminal configuration parameters	*page 6-383*
timezone	Displays timezone information for the system and managed devices	*page 6-384*
upgrade-status	Displays image upgrade status	*page 6-384*
version	Displays a device's software and hardware version	*page 6-385*
vrrp	Displays *Virtual Router Redundancy Protocol* (VRRP) protocol details	*page 6-386*
what	Displays details of a specified search phrase	*page 6-387*
wireless	Displays wireless configuration parameters	*page 6-388*
wwan	Displays the wireless WAN status	*page 6-401*

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

```
rfs7000-37FABE(config)#show ?
  adoption                    Display information related to adoption to
                              wireless controller
  advanced-wips               Advanced WIPS
  ap-upgrade                  AP Upgrade
  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
  dot1x                       802.1X
  event-history               Display event history
  event-system-policy         Display event system policy
  file                        Display filesystem information
  firewall                    Wireless Firewall
  interface                   Interface Configuration/Statistics commands
  ip                          Internet Protocol (IP)
  ip-access-list-stats        IP Access list stats
  l2tpv3                      L2TPv3 information
  licenses                    Show installed licenses and usage
  lldp                        Link Layer Discovery Protocol
  logging                     Show logging information
  mac-access-list-stats       MAC Access list stats
  mac-address-table           Display MAC address table
  mint                        MiNT protocol
  noc                         Noc-level information
  ntp                         Network time protocol
  password-encryption         Pasword encryption
  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
  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(config)#

rfs7000-37FABE(config)#show clock
2012-05-28 12:52:55 UTC
rfs7000-37FABE(config)#
```

PRIVILEGE EXEC Mode

```
rfs7000-37FABE#show ?
  adoption                    Display information related to adoption to
```

```
                                wireless controller
  advanced-wips                 Advanced WIPS
  ap-upgrade                    AP Upgrade
  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
  dot1x                         802.1X
  event-history                 Display event history
  event-system-policy           Display event system policy
  file                          Display filesystem information
  firewall                      Wireless Firewall
  interface                     Interface Configuration/Statistics commands
  ip                            Internet Protocol (IP)
  ip-access-list-stats          IP Access list stats
  l2tpv3                        L2TPv3 information
  licenses                      Show installed licenses and usage
  lldp                          Link Layer Discovery Protocol
  logging                       Show logging information
  mac-access-list-stats         MAC Access list stats
  mac-address-table             Display MAC address table
  mint                          MiNT protocol
  noc                           Noc-level information
  ntp                           Network time protocol
  password-encryption           Pasword encryption
  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
  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#

rfs7000-37FABE#show terminal
```

```
Terminal Type: xterm
Length: 24     Width: 80
rfs7000-37FABE#
```

USER EXEC Mode

```
rfs7000-37FABE>show ?
  adoption                    Display information related to adoption to
                              wireless controller
  advanced-wips               Advanced WIPS
  ap-upgrade                  AP Upgrade
  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
  dot1x                       802.1X
  event-history               Display event history
  event-system-policy         Display event system policy
  firewall                    Wireless Firewall
  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
  mint                        MiNT protocol
  noc                         Noc-level information
  ntp                         Network time protocol
  password-encryption         Pasword encryption
  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
  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

rfs7000-37FABE>
```

```
rfs7000-37FABE>show wireless ap configured
--------------------------------------------------------------------------------
--------
 IDX      NAME             MAC            PROFILE      RF-DOMAIN    ADOPTED-BY
--------------------------------------------------------------------------------
--------
  1   br71xx-139B34   00-23-68-13-9B-34   default-br71xx   default
un-adopted
  2   br7131-4AA708   00-04-96-4A-A7-08   default-br71xx   default
un-adopted
  3   br71xx-889EC4   00-15-70-88-9E-C4   default-br71xx   default
un-adopted
  4   br650-000001    00-A0-F8-00-00-01   default-br650    default
un-adopted
  5   br650-000010    00-A0-F8-00-00-10   default-br650    default
un-adopted
  6   br650-311641    00-23-68-31-16-41   default-br650    default
un-adopted
--------------------------------------------------------------------------------
--------
rfs7000-37FABE>
```

adoption

show commands

The adoption command is common to all three modes.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
show adoption [config-errors|history|info|offline|pending|status]

show adoption offline
show adoption config-errors <DEVICE-NAME>
show adoption [history|info|pending|   status] {on <DEVICE-NAME>}
```

Parameters

```
show adoption offline
```

adoption	Displays AP adoption history and status. 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 AP adoption history and status. It also displays configuration errors.
config-errors <DEVICE-NAME>	Displays configuration errors for a specified adopted access point or all access points adopted by a specified wireless controller • <DEVICE-NAME> – Specify the name of the AP or wireless controller.

	show adoption [history|info|pending| status] *{on <DEVICE-NAME>}*
adoption	Displays AP adoption history and status. It also displays configuration errors.
history	Displays the adoption history of the logged device and its adopted access points
info	Displays adopted device information
pending	Displays pending device adoption information
status	Displays adoption status for logged devices
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 or wireless controller.

Example

```
rfs7000-37FABE>show adoption offline
-------------------------------------------------------------------------------
----------
         MAC            HOST-NAME         TYPE        RF-DOMAIN             TIME
OFFLINE
-------------------------------------------------------------------------------
----------
 00-A0-F8-00-00-01        br650-000001    br650            default
unknown
 00-04-96-4A-A7-08       br71xx-4AA708   br71xx           default
unknown
 00-A0-F8-CF-1E-DA        br300-CF1EDA    br300         (un-mapped)
unknown
-------------------------------------------------------------------------------
----------
Total number o APs displayed: 3
rfs7000-37FABE>
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
show advanced-wips [configuration|stats]

show advanced-wips configuration [events {thresholds}|terminate-list]

show advanced-wips stats
[ap-table|client-table|connected-sensors|detected-aps|
          detected-clients-for-ap|event-history|server-listening-port]
```

```
show advanced-wips stats [ap-table|client-table|connected-sensors|
event-history|
          server-listening-port]
show advanced-wips stats [detected-aps|detected-clients-for-ap <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 are assigned to wireless controllers and 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
[ap-table|client-table|connected-sensors|event-history|
server-listening-port]
```

stats	Displays advanced WIPS statistics
ap-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 AP <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-ap <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-ap      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)#
```

ap-upgrade

show commands

Displays AP firmware image upgrade information, such as upgrade history, status, and image version

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
show ap-ugrade [history|load-image-status|status|versions]
```

```
show ap-upgrade [history {on <RF-DOMAIN-NAME>}|load-image-status|
          status {on [<RF-DOMAIN-NAME>|<RF-DOMAIN-MANAGER>]}|
          versions {on <RF-DOMAIN-MANAGER>}]
```

Parameters

```
show ap-upgrade [history {on <RF-DOMAIN-NAME>}|load-image-status|
status {on [<RF-DOMAIN-NAME>|<RF-DOMAIN-MANAGER>]}|versions {on
<RF-DOMAIN-MANAGER>}]
```

ap-upgrade	Displays AP firmware upgrade details, such as history, status, and version
history {on <RF-DOMAIN-NAME>}	Displays AP firmware upgrade history (AP address, upgrade result, time of upgrade, number of retries, upgraded by etc.) • on <RF-DOMAIN-NAME> – Optional. Displays AP firmware upgrade history on a specified RF Domain • <RF-DOMAIN-NAME> – Specify the RF Domain name.
load-image-status	Displays firmware image download status on the logged device
status {on [<RF-DOMAIN-NAME>|<RF-DOMAIN-MANAGER>]}	Displays AP firmware upgrade status • on – Optional. Displays firmware upgrade status on a specified RF Domain or RF Domain manager • <RF-DOMAIN-NAME> – Specify the RF Domain name. • <RF-DOMAIN MANAGER> – Specify the RF Domain manager name.
versions {on <RF-DOMAIN-MANAGER>}	Displays upgrade image versions • on <RF-DOMAIN-MANAGER> – Optional. Displays upgrade image versions on devices adopted by a specified RF Domain manager • <RF-DOMAIN MANAGER> – Specify the RF Domain manager name.

Example

```
rfs7000-37FABE>show ap-upgrade versions
-------------------------------------------------------------------------------
---
           CONTROLLER                AP-TYPE                  VERSION
-------------------------------------------------------------------------------
---
  00-15-70-37-FA-BE              br650              5.4.0.0-023D
  00-15-70-37-FA-BE              br71xx             none
  00-15-70-37-FA-BE              br6511             none
-------------------------------------------------------------------------------
---
rfs7000-37FABE>

rfs7000-37FABE(config)#show ap-upgrade history
-------------------------------------------------------------------------------
--------------------
               AP      RESULT                TIME  RETRIES        UPGRADED-BY
LAST-UPDATE-ERROR
-------------------------------------------------------------------------------
--------------------

 00-A0-F8-00-00-01       done  2010-11-22 14:14:09       0  00-15-70-37-FA-BE
-

 00-A0-F8-00-00-10       done  2010-12-05 10:50:14       0  00-15-70-37-FA-BE
-

 00-A0-F8-00-00-10       done  2010-12-05 15:07:25       0  00-15-70-37-FA-BE
-
```

```
 00-A0-F8-00-00-10       done  2011-01-08 13:15:19       0  00-15-70-37-FA-BE
-

 00-A0-F8-00-00-01       done  2011-01-08 13:22:19       0  00-15-70-37-FA-BE
-

 00-A0-F8-00-00-10       done  2011-01-08 13:50:02       0  00-15-70-37-FA-BE
-

 00-A0-F8-00-00-10       done  2011-01-08 14:20:20       0  00-15-70-37-FA-BE
-

 00-A0-F8-00-00-01       done  2011-01-08 15:21:38       0  00-15-70-37-FA-BE
-

 00-A0-F8-00-00-01     failed  2011-01-08 18:37:34       3  00-15-70-37-FA-BE
Reboot failed, retries = 3

 00-A0-F8-00-00-01     failed  2011-01-08 18:41:16       0  00-15-70-37-FA-BE
socket connection timed out

 00-A0-F8-00-00-01       done  2011-01-09 07:24:47       1  00-15-70-37-FA-BE
Reboot failed, retries = 0

 00-A0-F8-00-00-01       done  2011-01-09 18:00:27       0  00-15-70-37-FA-BE
-
--More--
```

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.

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 or wireless controller. Use the *on <DEVICE-NAME>* option to view a remote device's boot configuration.

Example

```
rfs7000-37FABE#show boot
------------------------------------------------------------------------------
---
     IMAGE            BUILD DATE             INSTALL DATE          VERSION
------------------------------------------------------------------------------
---
  Primary       2012-06-21 11:32:19     2012-06-26 14:29:03     5.4.0.0-023D
  Secondary     2012-05-23 13:00:02     2012-05-28 14:59:20     5.4.0.0-015D
------------------------------------------------------------------------------
---
Current Boot       : Primary
Next Boot          : Primary
Software Fallback  : Enabled
rfs7000-37FABE#
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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, 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

```
rfs7000-37FABE(config)#show captive-portal client on rfs7000-37FABE
------------------------------------------------------------------------------
----------
 CLIENT          IP       CAPTIVE-PORTAL        WLAN      VLAN    STATE
SESSION TIME
------------------------------------------------------------------------------
----------
------------------------------------------------------------------------------
----------
Total number of captive portal clients displayed: 0
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show captive-portal client statistics
------------------------------------------------------------------------------
---------------------------------
      CLIENT           IP        CAPTIVE-PORTAL     TX-PKTS     TX-BYTES
RX-PKTS        RX-BYTES
------------------------------------------------------------------------------
---------------------------------
------------------------------------------------------------------------------
---------------------------------
Total number of captive portal clients displayed: 0
rfs7000-37FABE(config)#
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 or wireless controller.
on <DEVICE-NAME>	Optional. Displays table details on a specified device • <DEVICE-NAME> – Specify the name of the AP or wireless controller.

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: 172.16.10.103
Platform: BR7131, Capabilites: Router Switch
Interface: ge1, Port ID (outgoing port): ge1
Hold Time: 174 sec

advertisement version: 2
Native VLAN: 1
Duplex: full
Version :
5.4.0.0-027B
-------------------------
Device ID: rfs4000-880DA7
Entry address(es):
  IP Address: 172.16.10.8
  IP Address: 192.168.0.1
Platform: RFS-4011-11110-US, Capabilites: Router Switch
Interface: ge1, Port ID (outgoing port): ge1
Hold Time: 122 sec

advertisement version: 2
--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  172.16.10.103 BR7131           ge1           ge1     full
 rfs4000-880DA7 172.16.10.8   RFS-4011-11110-US ge1          ge1     full
 rfs6000-380649 192.168.0.1   RFS6000           ge1          ge1     full
 br7131-139B34  172.16.10.22  BR7131N           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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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, or RF Domain.

Example

```
rfs7000-37FABE(config)#show clock
2012-04-11 10:18:02 UTC
rfs7000-37FABE(config)#
```

cluster

show commands

Displays cluster information (cluster configuration parameters, members, status etc.)

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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
5.4.0.0-146545X
------------------------------------------------------------------------------
---                             -------------------------
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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
show commands
```

Parameters

None

Example

```
rfs7000-37FABE(config)#show commands
  help
  help search WORD (|detailed|only-show|skip-show|skip-no)
  show commands
  show debugging (|(on DEVICE-OR-DOMAIN-NAME))
  show debugging cfgd
  show debugging fib(|(on DEVICE-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 mint (|(on DEVICE-OR-DOMAIN-NAME))
  show debugging mstp (|(on DEVICE-OR-DOMAIN-NAME))
  show debugging nsm (|(on DEVICE-OR-DOMAIN-NAME))
  show debugging advanced-wips
  show debugging vpn(|(on DEVICE-OR-DOMAIN-NAME))
  show debugging radius (|(on DEVICE-NAME))
  show debugging ospf(|(on DEVICE-NAME))
  show debugging zebra(|(on DEVICE-NAME))
  show debugging vrrp(|(on DEVICE-OR-DOMAIN-NAME))
  show debugging l2tpv3 (|(on DEVICE-OR-DOMAIN-NAME))
  show (running-config|session-config) (|include-factory)
  show running-config interface (|`WORD|ge <1-4>|me1|port-channel <1-2>|
          wwan1|pppoe1|vlan <1-4094>') (|include-factory)
  show running-config (aaa-policy AAA-POLICY|association-acl-policy
ASSOC-ACL|auto-provisioning-policy
AUTO-PROVISIONING-POLICY|captive-portal-policy CAPTIVE-PORTAL|dhcp---More---
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

```
rfs7000-37FABE(config)#show context
!
! Configuration of RFS7000 version 5.4.0.0-023D
!
!
version 2.1
!
!
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"
 permit any any type arp rule-precedence 20 rule-description "permit all ARP
traffic"
!
firewall-policy default
 no ip dos tcp-sequence-past-window
!
!
mint-policy global-default
!
meshpoint-qos-policy default
!
wlan-qos-policy default
 qos trust dscp
 qos trust wmm
!
radio-qos-policy default
!
--More--
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 or wireless controller.

Example

```
rfs4000-22CDAA(config)#show critical-resources on rfs4000-22CDAA
-------------------------------------------------------------------------
CRITICAL RESOURCE IP        VLAN          PING-MODE            STATE
-------------------------------------------------------------------------
172.168.1.103                1             arp-icmp             up
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
show crypto [ike|ipsec|key|pki]

show crypto ike sa {on|peer|version}
show crypto ike sa {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 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 {peer <IP>} {on <DEVICE-NAME>}`

crypto ike sa	Displays *Internet Key Exchange* (IKE) *security association* (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 or wireless controller.

`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 or wireless controller.

`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 or wireless controller.

`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 or wireless controller.

`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 or wireless controller.

`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 or wireless controller.

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=Morotola Inc
    Issuer Name:
      CN=70.37.fa.be:2010-04-26-15-00-39, C=US, O=Morotola Inc
    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=Morotola Inc
    Issuer Name:
      CN=70.37.fa.be:2010-04-26-15-00-39, C=US, O=Morotola Inc
    Valid From : Mon Apr 26 15:00:39 2010 UTC
    Valid Until: Tue Apr 26 15:00:39 2011 UTC
--More--
```

debug

show commands

Displays debugging status of the DPD2 module, profile functions, and XPath operations

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
show debug [profile|xpath]

show debug profile <WORD> {arg <WORD>}

show debug xpath [count|get|list]

show debug xpath [count|list] <WORD>

show debug xpath get <WORD> {option|param <WORD> option} [do-profiling|
no-pretty|
          show-tail-only|use-generator|use-streaming]
```

Parameters

```
show debug profile <WORD> {arg <WORD>}
```

debug profile <WORD> {arg <WORD>}	Displays profile function debugging status • <WORD> – Specify the name of the profile function (for example, mymodule.foo). • arg <WORD> – Optional. Specify arguments for the function in a single word, separated by a comma (for example. cli,[3,4]).

```
show debug xpath [count|list] <WORD>
```

debug xpath	Displays XPath-based operation debugging status

count <WORD>	Prints the number of items under an XPath node • <WORD> – Specify the XPath node. (for example, /wing-stats/device/self/interface)
list <WORD>	Lists the names (keys) under an XPath node • <WORD> – Specify the XPath node. (for example, /wing-stats/device/self/interface)

```
show debug xpath get <WORD> {option|param <WORD> option}
[do-profiling|no-pretty|
show-tail-only|use-generator|use-streaming]
```

debug xpath	Displays XPath-based operation debugging status
get <WORD>	Prints the XPath node value based on the options passed • <WORD> – Specify the XPath node. (for example, /wing-stats/device/self/interface)
option	Optional. Prints the XPath node value based on the options passed Select one of the following options: • do-profiling – Performs profiling • no-pretty – Disables pretty for speed • show-tail-only – Displays only the tail of the result • use-generator – Performs streaming using generator interface • use-streaming – Uses streaming interface
param <WORD> option	Optional. Prints the XPath node value based on the options passed • <WORD> – Specify the parameter in the dictionary format (for example, rf_domain_name:a_name,dummy_name:dummy_value) • option – After entering the parameter, select one of the following options: • do-profiling – Performs profiling • no-pretty – Disables pretty for speed • show-tail-only – Displays only the tail of the result • use-generator – Performs streaming using generator interface • use-streaming – Uses streaming interface

Example

```
rfs7000-37FABE(config)#show debug xpath count /wing-stats
Success: 4
rfs7000-37FABE(config)#

rfs7000-37FABE(config)*#show debug xpath get /wing-stats option do-profiling
no-pretty
exception [Traceback (most recent call last):
  File "/data/wing5.3-trunk/obj/qs5/src/sys/cfgd/debugcli.py", line 271, in
debug_xpath_get
  File "/data/wing5.3-trunk/obj/qs5/src/sys/cfgd/debugcli.py", line 259, in
debug_xpath_get_stats
  File "/usr/lib/python2.5/cProfile.py", line 30, in run
  File "/usr/lib/python2.5/cProfile.py", line 136, in run
  File "/usr/lib/python2.5/cProfile.py", line 141, in runctx
  File "<string>", line 1, in <module>
  File "/data/wing5.3-trunk/obj/qs5/src/sys/cfgd/debugcli.py", line 233, in
debug_xpath_get_stats_body
 File "/data/wing5.3-trunk/obj/qs5/src/sys/cfgd/core/cluster_db_api.py", line
61, in cluster_db_get_api
  File "/data/wing5.3-trunk/obj/qs5/src/sys/cfgd/core/cluster_db.py", line
517, in controlled_get
  File "/data/wing5.3-trunk/obj/qs5/src/sys/cfgd/core/cluster_db.py", line
485, in db_evaluate_core
  File "/data/wing5.3-trunk/obj/qs5/src/sys/cfgd/core/cluster_db.py", line
602, in cluster_db_evaluate_device
```

```
  File "/data/wing5.3-trunk/obj/qs5/src/sys/cfgd/core/datastore.py", line 354,
in evaluate
  File "/data/wing5.3-trunk/obj/qs5/src/sys/cfgd/core/datastore.py", line 284,
in evaluate
--More--

rfs7000-37FABE(config)#show debug xpath list /wing-stats
Success: ['device', 'rf_domain', 'noc']
rfs7000-37FABE(config)#
```

debugging

show commands

Displays debugging information. Use this command to confirm the status (enabled/disabled) of the various debugging processes supported.

NOTE
To enable debugging of various system modules, use the *debug* command in the USER EXEC or PRIV EXEC modes.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
show debugging
{advanced-wips|captive-portal|cfgd|dhcpsvr|fib|l2tpv3|mint|mstp|
          nsm|on|ospf|radius|snmp|ssm|voice|vpn|vrrp|wireless|zebra}

show debugging {advanced-wips|cfgd}
show debugging {captive-portal|l2tpv3|mint|mstp|nsm|voice|vpn|vrrp|wireless}
          {on <DEVICE-OR-DOMAIN-NAME>}
show debugging {on <DEVICE-OR-DOMAIN-NAME>}
show debugging {dhcpsvr|fib|ospf|radius|snmp|ssm|zebra} {on <DEVICE-NAME>}
```

Parameters

```
show debugging {advanced-wips|cfgd}
```

debugging {advanced-wips|cfgd}	Displays debugging processes in progress based on the parameters passed • advanced-wips – Optional. Displays the advanced WIPS module's debugging configuration • cfgd – Optional. Displays the cfgd process debugging configuration

`show debugging {captive-portal|l2tpv3|mint|mstp|nsm|voice|vpn|vrrp|wireless} {on <DEVICE-OR-DOMAIN-NAME>}`

debugging {captive-portal|l2tpv3|mint|mstp|nsm|voice|vpn|vrrp|wireless}	Displays debugging processes in progress based on the parameters passed • captive-portal – Optional. Displays the *hotspot* (HSD) module's debugging configuration • l2tpv3 – Optional. Displays the L2TPV3 module's debugging configuration • mint – Optional. Displays the MiNT module's debugging configuration • mstp – Optional. Displays the MST module's debugging configuration • nsm – Optional. Displays *Network Service Module* (NSM) debugging configuration • voice – Optional. Displays the voice module's debugging configuration • vpn – Optional. Displays the VPN module's debugging configuration • vrrp – Optional. Displays the *Virtual Router Redundancy Protocol* (VRRP) module's debugging configuration • wireless – Optional. Displays the wireless module's debugging configuration
on <DEVICE-OR-DOMAIN-NAME>	The following keyword is common to all of the above parameters: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays debugging processes on a device or RF Domain. • <DEVICE-OR-DOMAIN-NAME> – The name of the AP, wireless controller, or RF Domain.

`show debugging {dhcpsvr|fib|ospf|radius|snmp|ssm|zebra} {on <DEVICE-NAME>}`

debugging {dhcpsvr|fib|ospf radius|snmp|ssm|zebra}	Displays debugging processes in progress based on the parameters passed • dhcpsvr – Optional. Displays the DHCP server configuration module's debugging information • fib – Optional. Displays *Forwarding Information Base* (FIB) debugging information • ospf – Optional. Displays *Open Shortest Path First* (OSPF) debug log information • radius – Optional. Displays the RADIUS server configuration module's debugging information • snmp – Optional. Displays the *Simple Network Management Protocol* (SNMP) module's debugging information • ssm – Optional. Displays the *Security Services Module* (SSM) module's debugging information • zebra – Optional. Displays Zserver debugging information
on <DEVICE-NAME>	The following keyword is common to all of the above parameters: • on <DEVICE-NAME> – Optional. Displays debugging processes on a specified device • <DEVICE-NAME> – Specify the name of the AP or wireless controller.

`show debugging {on <DEVICE-OR-DOMAIN-NAME>}`

debugging {on <DEVICE-OR-DMAIN-NAME>}	Displays all debugging processes in progress on a specified device or RF Domain. • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays debugging processes in progress, on a device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, or RF Domain.

Example

```
rfs7000-37FABE(config)#show debugging cfgd
cfgd:
        config debugging is on
        cluster debugging is on
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show debugging radius
Radius:
        Debugging is enabled at level - RADIUS is not running
rfs7000-37FABE(config)#
```

dot1x

show commands

Displays dot1x information on interfaces

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
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 or wireless controller.
dot1x {on <DEVICE-NAME>}	Optional. Displays dot1x information for interfaces on a specified device • <DEVICE-NAME> – Specify the name of AP or wireless controller.

`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 or wireless controller

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)#
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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, or RF Domain.

Example

```
rfs7000-37FABE(config)#show event-history on rfs7000-37FABE
EVENT HISTORY REPORT
```

```
Generated on '2012-06-26 18:02:47 IST' by 'admin'

2012-06-26 17:18:34     rfs7000-37FABE  SYSTEM     LOGIN
Successfully logged in User: 'admin' with privilege 'superuser' from 'ssh'
2012-06-26 17:17:56     rfs7000-37FABE  SYSTEM     LOGOUT              Logged
out User: 'admin' with privilege 'superuser' from '172.16.10.12'
2012-06-26 16:47:04     rfs7000-37FABE  SYSTEM     LOGIN
Successfully logged in User: 'admin' with privilege 'superuser' from 'ssh'
2012-06-26 16:36:35     rfs7000-37FABE  SYSTEM     LOGOUT              Logged
out User: 'admin' with privilege 'superuser' from '172.16.10.12'
2012-06-26 16:06:27     rfs7000-37FABE  SYSTEM     LOGIN
Successfully logged in User: 'admin' with privilege 'superuser' from 'ssh'
2012-06-26 16:02:24     rfs7000-37FABE  SYSTEM     LOGOUT              Logged
out User: 'admin' with privilege 'superuser' from '172.16.10.12'
2012-06-26 14:42:00     rfs7000-37FABE  SYSTEM     LOGOUT              Logged
out User: 'admin' with privilege 'superuser' from '172.16.10.10'
2012-06-26 14:41:30     rfs7000-37FABE  SYSTEM     LOGIN
Successfully logged in User: 'admin' with privilege 'superuser' from 'ssh'
2012-06-26 14:40:37     rfs7000-37FABE  SYSTEM     LOGIN
Successfully logged in User: 'admin' with privilege 'superuser' from 'ssh'
2012-06-26 14:32:44     rfs7000-37FABE  DIAG       NEW_LED_STATE        LED
state message AP_LEDS_ON from module DOT11
2012-06-26 14:32:44     rfs7000-37FABE  DIAG       NEW_LED_STATE        LED
state message LED_ACTIVE_ADOPTING from module CFGD
--More--
rfs7000-37FABE(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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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.

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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
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 or wireless controller.

`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 or wireless controller.
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 or wireless controller.

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 or wireless controller.

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  rfs7000-37FABE
Active Flows       2
TCP flows          1
UDP flows          0
DHCP flows         1
ICMP flows         0
IPsec flows        0
L3/Unknown flows   0
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 or wireless controller.

Example

```
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)#
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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|me|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 or wireless controller.

`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 or wireless controller.

`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 or wireless controller

`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 or wireless controller.

`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
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 or wireless controller.

`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 or wireless controller.

	`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 or wireless controller.

	`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
<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 or wireless controller.

	`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 or wireless controller.

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)#
```

ip-access-list-stats

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
show ip-access-list-stats {<IP-ACCESS-LIST-NAME>} {(on <DEVICE-NAME>)}
```

Parameters

```
show ip-access-list-stats {<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.
on <DEVICE-NAME>	The following keyword is recursive and common to the 'IP-ACCESS-LIST-NAME' parameter: • 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 or wireless controller.

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
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 or wireless controller.

`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 or wireless controller.

`l2tpv3 {tunnel-summary} {on <DEVICE-NAME>}`

l2tpv3	Displays L2TPV3 tunnel and session details or summary
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 or wireless controller.

`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 or wireless controller.

Example

```
rfs7000-37FABE(config)#show l2tpv3
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show l2tpv3 tunnel-summary
Session Name : 1
 VLANs : 11 10 13 12 14 9
 Pseudo Wire Type : Ethernet_VLAN
 Serial number for the session : 31
 Local Session ID : 267330235
 Remote Session ID : 27841566
 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 : 109
 Trunk Session : 1
 Native VLAN tagged : 0
 Native VLAN ID : 9
 Number of packets received : 0
 Number of bytes received : 0
```

```
 Number of packets sent : 994
 Number of bytes sent : 93804
 Number of packets dropped : 0
rfs7000-37FABE(config)#
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
show licenses
```

Parameters

None

Example

```
rfs7000-37FABE(config)#show licenses
Serial Number : 6268529900014

Device Licenses:
  AP-LICENSE
    String     :
8088bb045018988b85bcd575d0ab7dbc802885bcc680a96194dfbeedc28d4117058eb53bd8b
    Value      : 50
    Used       : 0
  AAP-LICENSE
    String     :
8088bb045018988bf98ff7127cda1d354bc689885fcc6b625b695384946d4117058eb53bd8b
    Value      : 50
    Used       : 0
rfs7000-37FABE(config)#
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 or wireless controller.

```
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 or wireless controller.

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 or wireless controller.

Example

```
rfs7000-37FABE(config)#show logging on rfs7000-37FABE
```

```
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 (108793 bytes):


Apr 12 09:47:19 2012: %DATAPLANE-4-DOSATTACK: IPSPOOF ATTACK:  Source IP is
Spoofed : Src IP : 157.235.208.207, Dst IP: 172.16.10.1, Src Mac:
5C-D9-98-4C-04-51, Dst Mac: 00-15-70-37-FA-BE, Proto = 17.
Apr 12 09:46:58 2012: %DATAPLANE-4-DOSATTACK: IPSPOOF ATTACK:  Source IP is
Spoofed : Src IP : 157.235.208.207, Dst IP: 172.16.10.1, Src Mac:
5C-D9-98-4C-04-51, Dst Mac: 00-15-70-37-FA-BE, Proto = 17.
Apr 12 09:46:22 2012: %DATAPLANE-4-DOSATTACK: IPSPOOF ATTACK:  Source IP is
Spoofed : Src IP : 157.235.208.207, Dst IP: 172.16.10.1, Src Mac:
5C-D9-98-4C-04-51, Dst Mac: 00-15-70-37-FA-BE, Proto = 17.
Apr 12 09:46:01 2012: %DATAPLANE-4-DOSATTACK: IPSPOOF ATTACK:  Source IP is
Spoofed : Src IP : 157.235.208.207, Dst IP: 172.16.10.1, Src Mac:
5C-D9-98-4C-04-51,
--More--
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 or wireless controller.

Example

```
rfs7000-37FABE(config)#show mac-access-list-stats on rfs7000-37FABE
rfs7000-37FABE(config)#
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 or wireless controller.

Example

```
rfs7000-37FABE(config)#show mac-address-table on rfs7000-37FABE
+------------+----------+-----------+-------------------------+-----------
|   BRIDGE   |   VLAN   |    PORT   |           MAC           |    STATE     |
+------------+----------+-----------+-------------------------+-----------
| 1          | 1        | ge1       | 00-50-DA-EE-B5-5C       | forward        |
| 1          | 1        | ge1       | 00-A0-F8-00-00-00       | forward        |
| 1          | 1        | ge1       | 00-02-B3-28-D1-55       | forward        |
| 1          | 1        | ge1       | 00-A0-F8-68-D5-5D       | forward        |
| 1          | 1        | ge1       | 00-50-DA-95-11-13       | forward        |
| 1          | 1        | ge1       | 00-15-70-38-06-53       | forward        |
| 1          | 1        | ge1       | 00-15-70-41-9F-7F       | forward        |
| 1          | 1        | ge1       | 00-15-70-88-9E-C4       | forward        |
+------------+----------+-----------+-------------------------+-----------
rfs7000-37FABE(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 71XX Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 or wireless controller.

```
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 or wireless controller

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)#
```

noc

show commands

Displays *Network Operations Center* (NOC) level information

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
show noc [client-list|device|domain]

show noc client-list
show noc device {filter} {offline|online|rf-domain [<DOMAIN-NAME>|not
<DOMAIN-NAME>]}
show noc domain [managers|statistics {details}]
```

Parameters

`show noc client-list`

noc client-list	Displays a list of clients at the NOC level

`show noc device {filter} {offline|online|rf-domain [<DOMAIN-NAME>|not <DOMAIN-NAME>]}`

noc device filter	Displays devices in a network • filter – Optional. Displays network devices Use additional filters to view specific details
offline	Optional. Displays offline devices
online	Optional. Displays online devices
rf-domain {<DOMAIN-NAME>| not <DOMAIN-NAME>}	Optional. Displays devices on a specified RF Domain • <DOMAIN-NAME> – Specify the name of the RF Domain. • not <DOMAIN-NAME> – Inverts the selection

`show noc domain [managers|statistics {details}]`

noc domain	Displays RF Domain information Use this command to view all domain managers and get RF Domain statistics

managers	Lists RF Domains and managers
statistics {details}	Displays RF Domains statistics • details – Optional. Provides detailed RF Domain statistics

Example

```
rfs7000-37FABE(config)#show noc device filter online
------------------------------------------------------------------------------
MAC    HOST-NAME     TYPE        CLUSTER      RF-DOMAIN       ADOPTED-BY
ONLINE
------------------------------------------------------------------------------
00-15-70-37-FA-BE rfs7000-37FABE rfs7000  RFDOMAI..echPubs             online
------------------------------------------------------------------------------
Total number of clients displayed: 1
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show noc device
------------------------------------------------------------------------------
---------------------------------
             MAC     HOST-NAME      TYPE         CLUSTER       RF-DOMAIN
ADOPTED-BY     ONLINE
------------------------------------------------------------------------------
---------------------------------
 00-A0-F8-00-00-01   br650-000001   br650                 default
offline
 00-15-70-37-FA-BE  rfs7000-37FABE rfs7000      test RFDOMAI..sLabLan
online
 00-04-96-4A-A7-08   br71xx-4AA708  br71xx                default
offline
 00-A0-F8-CF-1E-DA   br300-CF1EDA   br300              (un-mapped)
offline
------------------------------------------------------------------------------
---------------------------------
Total number of clients displayed: 4
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show noc domain statistics details
==============================================================================
RF-Domain RFDOMAIN_UseCase1
Note: TX = AP->Client, RX = Client->AP
------------------------------------------------------------------------------
Data bytes            : ( TX + RX = Total ),  0 + 0 = 0  bytes
Data throughput       : ( TX + RX = Total ),  0 Kbps + 0 Kbps = 0 Kbps
Data packets          : ( TX + RX = Total ),  0 + 0 = 0 pkts
Data pkts/sec         : ( TX + RX = Total ),  0 + 0 = 0 pps
BCMC Packets          : ( TX + RX = Total ),  0 + 0 = 0 pkts
Management Packets    : ( TX + RX = Total ),  0 + 0 = 0 pkts
Packets Discarded     : 0 - Tx Dropped, 0 - Rx Errors
Indicators            : T = 0 @ Max user rate of 0 Kbps
Distribution          : 0 Clients, 0 radios
Client count Detais   : 0/0/0 (b/bg/bgn); 0/0 (a/an)
Stats Update Info     : 6 seconds - update interval, mode is auto
Threat Level          : 0
Cause of concern      :
Remedy                :
Last update           : 2010-01-31 10:30:22 by 00-15-70-37-FA-BE
------------------------------------------------------------------------------

Total number of RF-domain displayed: 1
```

```
rfs7000-37FABE(config-rf-domain-RFDOMAIN_UseCase1)#

rfs7000-37FABE(config)#show noc domain statistics details
==========================================================================
RF-Domain RFDOMAIN_TechPubs
Note: TX = AP->Client, RX = Client->AP
--------------------------------------------------------------------------
Data bytes            : ( TX + RX = Total ),  0 + 0 = 0  bytes
Data throughput       : ( TX + RX = Total ),  0 Kbps + 0 Kbps = 0 Kbps
Data packets          : ( TX + RX = Total ),  0 + 0 = 0 pkts
Data pkts/sec         : ( TX + RX = Total ),  0 + 0 = 0 pps
BCMC Packets          : ( TX + RX = Total ),  0 + 0 = 0 pkts
Management Packets    : ( TX + RX = Total ),  0 + 0 = 0 pkts
Packets Discarded     : 0 - Tx Dropped, 0 - Rx Errors
Indicators            : T = 0 @ Max user rate of 0 Kbps
Distribution          : 0 Clients, 0 radios
Client count Detais   : 0/0/0 (b/bg/bgn); 0/0 (a/an)
Stats Update Info     : 6 seconds - update interval, mode is auto
Threat Level          : 1
Cause of concern      : no sensors enabled in RF-domain RFDOMAIN_TechPubs
Remedy                : enable AP detection
Last update           : 2011-01-09 08:44:15 by 00-15-70-37-FA-BE
--------------------------------------------------------------------------

Total number of RF-domain displayed: 1
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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 or wireless controller.
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 or wireless controller.

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 or wireless controller.

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
show reload {on <DEVICE-NAME>}
```

Parameters

```
show reload {on <DEVICE-NAME>}
```

reload {on <DEVICE-NAME>}	Displays scheduled reload information for a specified device • on <DEVICE-NAME> – Optional. Displays configuration on a specified device • <DEVICE-NAME> – Specify the name of the AP or wireless controller.

Example

```
rfs7000-37FABE(config)#show reload on rfs7000-37FABE
No reload is scheduled.
rfs7000-37FABE(config)#
```

remote-debug

show commands

Displays remote debug session information

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
show remote-debug
```

Parameters

None

Example

```
rfs7000-37FABE(config)#show remote-debug
live-pktcap
 Not running
wireless
 Not running
copy-crashinfo
 Not running
offline-pktcap
 Not running
copy-techsupport
 Not running
more
 Not running
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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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, 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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 For more information on route maps, see *route-map on page 26-993*
on <DEVICE-NAME>	Optional. Displays route map statistics on a specified device • <DEVICE-NAME> – Specify the name of the AP or wireless controller.

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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, or RF Domain.

Example

```
rfs7000-37FABE(config)#show rtls aeroscout on rfs7000-37FABE
Total number of APs displayed: 0
rfs7000-37FABE(config)#
```

running-config

show commands

Displays configuration files (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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
show running-config {aaa-policy|association-acl-policy|auto-provisioning-
policy|
          captive-portal-policy|device|dhcp-server-policy|firewall-policy|
include-factory|
          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 [br650|br6511|br71xx|
          rfs4000|rfs6000|rfs7000] <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|br71xx|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.
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.
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)
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

```
rfs7000-37FABE(config)#show session-config
!
! Configuration of Brocade Mobility RFS7000 version 5.4.0.0-027B
!
!
version 2.1
!
!
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 test
!
mac access-list PERMIT-ARP-AND-IPv4
 permit any any type ip rule-precedence 10 rule-description "permit all IPv4
traffic"
--More--
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 or wireless controller.

Example

```
rfs7000-37FABE#show sessions
INDEX   COOKIE  NAME            START TIME              FROM                 ROLE
1       5       snmp             2012-06-26 13:23:11     127.0.0.1
superuser
2       6       snmp2            2012-06-26 13:23:11     127.0.0.1
superuser
3       10      admin            2012-06-27 14:11:53     172.16.10.12
superuser

rfs7000-37FABE#
```

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 71XX Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
show smart-rf [ap|calibration-config|calibration-status|channel-distribution|

history|history-timeline|interfering-ap|interfering-neighbors|radio]

show smart-rf ap {<MAC>|<DEVICE-NAME>|activity|energy|neighbors|on
<DOMAIN-NAME>}
show smart-rf ap {<MAC>|<DEVICE-NAME>} {on <DOMAIN-NAME>}
show smart-rf ap (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 radio {activity|neigbors}{<MAC>|all-11an|all-11bgn} {on <DOMAIN-
NAME>}

show smart-rf interfering-ap {<MAC>|<DEVICE-NAME>|on}

show smart-rf interfering-neighbors {<MAC>|<DEVICE-NAME>|on|threshold
<50-100>}
```

Parameters

```
show smart-rf ap {<MAC>|<DEVICE-NAME>} {on <DOMAIN-NAME>}
```

ap	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 ap (activity|energy|neighbors} [<MAC>|<DEVICE-NAME>]
{(on <DOMAIN-NAME>)}
```

ap	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-ap {<MAC>|<DEVICE-NAME>|on}`

interfering-ap	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. 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. 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-ap	Displays interfering neighboring access point information
<MAC>	Optional. Displays interfering neighboring access point information • <MAC> – Specify the access point's MAC address. 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. 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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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. • me1 – Displays FastEthernet interface MST configuration • port-channel – Displays port channel interface MST configuration • <1-2> – Select the port channel interface index from 1 - 2. • 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 or wireless controller.

`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 or wireless controller.

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)#
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

```
rfs7000-37FABE(config)#show startup-config
!
! Configuration of Brocade Mobility RFS7000 version 5.4.0.0-027B
!
!
version 2.1
!
!
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 test
!
mac access-list PERMIT-ARP-AND-IPv4
 permit any any type ip rule-precedence 10 rule-description "permit all IPv4
traffic"
--More--
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 or wireless controller.

Example

```
rfs7000-37FABE(config)#show upgrade-status detail on rfs7000-37FABE
Last Image Upgrade Status : Successful
Last Image Upgrade Time   : 2012-06-26 14:29:03
rfs7000-37FABE(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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 or wireless controller.

Example

```
rfs7000-37FABE(config)#show version on rfs7000-37FABE
Brocade Mobility RFS7000 version 5.4.0.0-023D
```

```
Copyright (c) 2004-2012 Inc. All rights reserved.
Booted from primary

rfs7000-37FABE uptime is 0 days, 19 hours 43 minutes
CPU is RMI XLR V0.4
Base ethernet MAC address is 00-15-70-37-FA-BE
System serial number is 6268529900014
Model number is RFS-7010-1000-WR
FPGA version is 3.41
rfs7000-37FABE(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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 or wireless controller.

```
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 or wireless controller.

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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, or RF Domain.

Example

```
rfs7000-37FABE#show what contain default on rfs7000-37FABE
--------------------------------------------------------------------------------
--------------------------------------------------------------------------
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          br650
00-A0-F8-00-00-01               default

                    https-trustpoint            type
mac                             rf_domain_name
2   device-cfg       default-trustpoint          rfs7000
00-15-70-37-FA-BE               RFDOMAIN_TechPubsLabLan

                    https-trustpoint            type
mac                             rf_domain_name
3   device-cfg       default-trustpoint          br71xx
00-04-96-4A-A7-08               default
--More--
rfs7000-37FABE#
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
show wireless
[ap|client|domain|mesh|meshpoint|radio|regulatory|sensor-server|
          unsanctioned|wips|wlan]

show wireless ap {configured|detail|load-balancing|on <DEVICE-NAME>}
show wireless ap {configured}
show wireless ap {detail} {<MAC/HOST-NAME>} {(on <DEVICE-OR-DOMAIN-NAME>)}
show wireless ap {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 domain statistics {detail} {(on <DEVICE-OR-DOMAIN-NAME>)}

show wireless mesh [detail|links]
show wireless mesh links {on <DEVICE-OR-DOMAIN-NAME>}
show wireless mesh detail {<DEVICE-NAME>|filter|on <DEVICE-OR-DOMAIN-NAME>}
show wireless mesh detail {<DEVICE-NAME>} {<1-3>|filter <RADIO-MAC>|on}
show wireless mesh detail {filter <RADIO-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 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 [br300|br650|br6511|
          br71xx|rfs4000] <WORD>

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 ap {configured}
```

wireless	Displays wireless configuration parameters
ap	Displays managed access point information
configured	Optional. Displays configured AP information, such as name, MAC address, profile, RF Domain and adoption status

```
show wireless ap {detail} {<MAC/HOST-NAME>} {(on <DEVICE-OR-DOMAIN-NAME>)}
```

wireless	Displays wireless configuration parameters
ap	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, or RF Domain.

```
show wireless ap {load-balancing} {client-capability|events|neighbors}
{(on <DEVICE-NAME)}
```

wireless	Displays wireless configuration parameters
ap	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 or wireless controller.

```
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, 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, 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, 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, or RF Domain.

	`show wireless domain statistics {detail} {(on <DEVICE-OR-DOMAIN-NAME>)}`
wireless	Displays wireless configuration parameters
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, or RF Domain.

	`show sireless mesh links {on <DEVICE-OR-DOMAIN-NAME>}`
wireless	Displays wireless configuration parameters
mesh	Displays radio mesh related information
links {on <DEVICE-OR-DOMAIN-NAME>}	Displays active radio mesh links • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays active radio mesh links on a specified device or RF Domain

`show wireless mesh detail {<DEVICE-NAME>} {<1-3>|filter <RADIO-MAC>|on}`

wireless	Displays wireless configuration parameters
mesh	Displays radio mesh information
detail	Displays detailed radio mesh information
<DEVICE-NAME>	Optional. Displays information for a specified mesh. Specify the MAC address or hostname, or append the interface number to form the mesh ID in the AA-BB-CC-DD-EE-FF:RX or HOSTNAME:RX format.
<1-3>	Optional. Specifies the mesh interface index (if not specified as part of the mesh 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, 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 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, 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, 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, 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-DOMAIN-NAME> – Specify the name of the AP, wireless controller, or RF Domain.
rf {on <DEVICE-OR-DOMAIN-NAME>}	Optional. Displays RF statistics on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, 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, 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, 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 [br300|br650|br71xx|rfs4000] <WORD>`

wireless	Displays wireless configuration parameters
regulatory	Displays wireless regulatory information
device-type [br300| br650|br6511|br71xx| rfs4000] <WORD>	Displays regulatory information based on the device type • br300 – Displays Brocade Mobility 300 Access Point information • br650 – Displays Brocade Mobility 650 Access Point information • br6511 – Displays Brocade Mobility 6511 Access Point information • br71xx – Displays Brocade Mobility 71XX Access Point information • rfs4000 – Displays Brocade Mobility RFS4000 information The following keyword is common to all of the above: • <WORD> – Specify the two letter ISO-3166 country code.

`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, 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, 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, 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 4-148*.

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)
-----------------------------------------------------------------------------
  1   1-13        4000      36          Indoor/Outdoor   NA             NA
  2   36-64       200       23          Indoor           Not Required   0
  3   149-165     1000      30          Outdoor          Not Required   0
  4   149-165     200       23          Indoor           Not Required   0
-----------------------------------------------------------------------------
rfs7000-37FABE(config)#
```

```
rfs4000-880DA7(config)#show wireless ap detail rfs4000-880DA7 on
rfs4000-880DA7
AP: 00-23-68-88-0D-A7
 AP Name              : rfs4000-880DA7
 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
rfs4000-880DA7(config)#

rfs4000-880DA7(config)#show wireless ap load-balancing on
default/rfs4000-880DA7

AP: 00-23-68-88-0D-A7
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
rfs4000-880DA7(config)#

rfs4000-880DA7(config)#show wireless ap 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
--------------------------------------------------------------------------------
rfs4000-880DA7   default    default 00-23-68-88-0D-A7  2  W-W    0
not done
--------------------------------------------------------------------------------
Total number of APs displayed: 1
rfs4000-880DA7(config)#

rfs4000-1B3596#show wireless meshpoint tree
1:c00466 [5 MPs(3 roots, 2 bound)]
|-br7131-96FAAC
```

```
| |-br7131-96F998
|   |-br7131-96F6B4
|-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#
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

```
rfs4000-880DA7(config-device-00-23-68-88-0D-A7)#show wwan configuration on
rfs4000-880DA7
>>> WWAN Configuration:
+----------------------------------------
|  Access Port Name : isp.cingular
|  User Name        : testuser
|  Cryptomap        : map1
+----------------------------------------
rfs4000-880DA7(config-device-00-23-68-88-0D-A7)#

rfs4000-880DA7(config-device-00-23-68-88-0D-A7)#show wwan status on
rfs4000-880DA7
>>> WWAN Status:
+----------------------------------------
|  State : ACTIVE
|  DNS1  : 209.183.54.151
|  DNS2  : 209.183.54.151
+----------------------------------------
rfs4000-880DA7(config-device-00-23-68-88-0D-A7)#

rfs7000-37FABE(config)#show wwan configuration on rfs7000-37FABE
>>> WWAN Configuration:
+----------------------------------------
|  Access Port Name : None
|  User Name        : None
+----------------------------------------

rfs7000-37FABE(config)#
```

Chapter

7

Profiles

In this chapter

Profiles enable administrators to assign a common set of configuration parameters and policies to wireless controllers and access points. Profiles can be used to assign common or unique network, wireless and security parameters to 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 wireless controller supports both default and user defined profiles implementing new features or updating existing parameters to groups of wireless controller or access points. 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 a wireless controller, and default AP profiles are applied to the APs automatically discovered by the wireless controller. After adoption, if a change is made in one of the parameters in the profile, that change is reflected across all the APs using the same profile.

User defined profiles are manually created for each supported wireless controller and access point model. User defined profiles can be manually assigned or automatically assigned to access points.

- Brocade Mobility 650 Access Point – Adds an Brocade Mobility 650 Access Point access point profile
- Brocade Mobility 71XX Access Point – Adds an Brocade Mobility 71XX 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

Each default and user defined profile contains policies and configuration parameters. Changes made to these parameters are automatically inherited by the devices assigned to the profile.

```
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)#
```

7

Profile Config Commands

NOTE
The commands present under ‘Profiles’ are also available under the ‘Device mode’. The additional commands specific to the ‘Device mode’ are listed separately. Refer *Chapter 7, <$elemtextDevice Config Commands* for more information.

Table 20 summarizes profile configuration commands.

TABLE 20 Profile-Config Commands

Command	Description	Reference
ap-mobility	Configures AP mobility (fixed or vehicle mounted). This command is applicable only to the AP profiles.	*page 7-406*
ap-upgrade	Enables automatic AP firmware upgrade	*page 7-406*
br300	Enables adoption of Brocade Mobility 300 Access Points	*page 7-407*
arp	Configures static address resolution protocol	*page 7-408*
auto-learn-staging-config	Enables network configuration learning of devices	*page 7-410*
autoinstall	Configures the automatic install feature	*page 7-410*
bridge	Configures bridge specific parameters	*page 7-412*
captive-portal	configures captive portal advanced Web page upload on a device profile	*page 7-424*
cdp	Enables *Cisco Discovery Protocol* (CDP) on a device	*page 7-424*
cluster	Configures a cluster name	*page 7-425*
configuration-persistence	Enables persistence of configuration across reloads	*page 7-427*
controller	Configures a wireless controller	*page 7-428*
critical-resource	Monitors user configured IP addresses and logs their status	*page 7-430*
crypto	Configures crypto settings	*page 7-432*
dot1x	Configures 802.1x standard authentication controls	*page 7-457*
dscp-mapping	Configures an IP DSCP to 802.1p priority mapping for untagged frames	*page 7-458*
email-notification	Configures e-mail notification	*page 7-459*
enforce-version	Checks device firmware versions before attempting connection	*page 7-460*
events	Displays system event messages	*page 7-461*
export	Enables export of startup.log file after every boot	*page 7-462*
interface	Configures an interface	*page 7-463*
ip	Configures IP components	*page 7-531*
l2tpv3	Defines the *Layer 2 Tunnel Protocol* (L2TP) protocol for tunneling Layer 2 payloads using *Virtual Private Networks* (VPNs)	*page 7-538*
l3e-lite-table	Configures L3e Lite Table with this profile	*page 7-539*
led	Turns device LEDs on or off	*page 7-540*
legacy-auto-downgrade	Auto downgrades a legacy device firmware	*page 7-541*

TABLE 20 Profile-Config Commands

Command	Description	Reference
legacy-auto-update	Auto upgrades a legacy device firmware	*page 7-541*
lldp	Configures *Link Layer Discovery Protocol* (LLDP)	*page 7-542*
load-balancing	Configures load balancing parameters	*page 7-543*
logging	Modifies message logging	*page 7-547*
mac-address-table	Configures the MAC address table	*page 7-549*
memory-profile	Configures the memory profile used on the device	*page 7-550*
meshpoint-device	Configures a meshpoint device parameters	*page 7-551*
meshpoint-monitor-interval	Configures meshpoint monitoring interval	*page 7-551*
min-misconfiguration-recovery-time	Configures the minimum wireless controller connectivity verification time	*page 7-552*
mint	Configures MiNT protocol	*page 7-553*
misconfiguration-recovery-time	Verifies wireless controller connectivity after a configuration is received	*page 7-556*
neighbor-inactivity-timeout	Configures neighbor inactivity timeout	*page 7-557*
neighbor-info-interval	Configures neighbor information exchange interval	*page 7-557*
no	Negates a command or reverts settings to their default	*page 7-558*
noc	Configures NOC settings	*page 7-561*
ntp	Configures an NTP server	*page 7-562*
power-config	Configures the power mode	*page 7-563*
preferred-controller-group	Specifies the wireless controller group preferred for adoption	*page 7-564*
preferred-tunnel-controller	Configures the tunnel wireless controller preferred by the system to tunnel extended VLAN traffic	*page 7-565*
radius	Configures device-level RADIUS authentication parameters	*page 7-566*
rf-domain-manager	Enables RF Domain manager	*page 7-567*
router	Configures dynamic router protocol settings	*page 7-568*
spanning-tree	Configures spanning tree commands	*page 7-569*
tunnel-controller	Configures the name of tunneled WLAN (extended VLAN) wireless controller	*page 7-571*
use	Uses pre configured policies with this profile	*page 7-572*
vrrp	Configures *Virtual Router Redundancy Protocol* (VRRP) group settings	*page 7-574*
wep-shared-key-auth	Enables support for 802.11 WEP shared key authentication	*page 7-577*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
do	Runs commands from the EXEC mode	*page 4-165*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*

TABLE 20 Profile-Config Commands

Command	Description	Reference
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes information to memory or terminal	*page 5-310*

ap-mobility

Profile Config Commands

Configures AP mobility (fixed or vehicle mounted)

NOTE
The ap-mobility command is applicable only to an access point profile.

Supported in the following platforms:

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

Syntax:

```
ap-mobility [fixed|vehicle-mounted]
```

Parameters

```
ap-mobility [fixed|vehicle-mounted]
```

fixed	Configures the access point profile for a fixed infrastructure device
vehicle-mounted	Configures the access point profile for a vehicle mounted device (a moving device)

Example

```
rfs7000-37FABE(config-profile-default-br71xx)#ap-mobility fixed
rfs7000-37FABE(config-profile-default-br71xx)#
```

Related Commands:

no	Disables or reverts settings to their default

ap-upgrade

Profile Config Commands

Enables an automatic firmware upgrade on an adopted access point

Supported in the following platforms:

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

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
ap-upgrade [auto|count]

ap-upgrade auto {(br650|br6511|br71xx)}

ap-upgrade count <1-20>
```

Parameters

```
ap-upgrade auto {(br650|br6511|br71xx)}
```

auto	Enables automatic firmware upgrade on an adopted AP
br650	Optional. Enables automatic Brocade Mobility 650 Access Point firmware upgrade
br6511	Optional. Enables automatic Brocade Mobility 6511 Access Point firmware upgrade
br71xx	Optional. Enables automatic Brocade Mobility 71XX Access Point firmware upgrade

```
ap-upgrade count <1-20>
```

count <1-20>	Sets a limit to the number of concurrent upgrades performed • <1-20> – Specify a value from 1 - 20.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#ap-upgrade count 7
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Disables automatic AP upgrade

br300

Profile Config Commands

Enables or disables adoption of an Brocade Mobility 300 Access Point by a profile or wireless controller

Supported in the following platforms:

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
br300 [<MAC>|adopt-unconfigured]
br300 <MAC> [adopt|deny]
br300 adopt-unconfigured
```

Parameters

	`br300 <MAC> [adopt|deny]`
br300	Adopts or denies adoption of an Brocade Mobility 300 Access Point. It also facilitates adoption of non-configured Brocade Mobility 300 Access Points.
<MAC> [adopt|deny]	Configures an Brocade Mobility 300 Access Point adopt or deny list, using the device's MAC address. Specify the Brocade Mobility 300 Access Point's MAC address. • adopt – Adds an Brocade Mobility 300 Access Point to the adopt list • deny – Adds an Brocade Mobility 300 Access Point to the deny list

	`br300 adopt-unconfigured`
br300	Adopts or denies adoption of an Brocade Mobility 300 Access Point. It also facilitates adoption of all non-configured Brocade Mobility 300 Access Points.
adopt-unconfigured	Adopts non-configured Brocade Mobility 300 Access Point devices

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#br300 00-15-70-63-4F-86

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
  qos trust 802.1p
 interface pppoe1
--More--
 use firewall-policy default
 br300 00-15-70-63-4F-86 adopt
 service pm sys-restart
 router ospf
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Dissociates (un maps) an Brocade Mobility 300 Access Point from the adopt or deny list. Also disables non-configured Brocade Mobility 300 Access Point adoption.

arp

Profile Config Commands

Adds a static *Address Resolution Protocol* (ARP) IP address in the ARP cache

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
arp [<IP>|timeout]
```

```
arp <IP> <MAC> arpa [<L3-INTERFACE-NAME>|pppoe1|vlan <1-4094>|wwan1]
          {dhcp-server|router}

arp timeout <15-86400>
```

Parameters

```
arp <IP> <MAC> arpa [<L3-INTERFACE-NAME>|pppoe1|vlan <1-4094>|wwan1]
{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 SVI.
arpa	Sets ARP encapsulation type to ARPA
<L3-INTERFACE-NAME>	Configures statics for a specified router interface • <L3-INTERFACE-NAME> – Specify the router interface name.
pppoe1	Configures statics for PPP over Ethernet interface
vlan <1-4094>	Configures statics for a VLAN interface • <1-4094> – Specify a SVI VLAN ID from 1 - 4094.
wwan1	Configures statics for Wireless WAN interface
{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--
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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--
```

Related Commands:

no	Disables the auto install settings

bridge

Profile Config Commands

Table 21 summarizes Ethernet bridge configuration commands.

TABLE 21 Bridge-Config Commands

Command	Description	Reference
bridge	Enables Ethernet bridge configuration context	*page 7-412*
bridge-vlan-mode commands	Summarizes bridge VLAN configuration mode commands	*page 7-413*

bridge

bridge

Configures VLAN Ethernet bridging parameters

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

NOTE
The interfaces mentioned below are supported as follows:
- ge <index> – Brocade Mobility RFS7000 and Brocade Mobility RFS4000 supports 4 GEs
- me1 – Only supported on Brocade Mobility RFS7000 and Brocade Mobility RFS6000

Syntax:

```
bridge [nat|vlan]

bridge nat source list <IP-ACCESS-LIST-NAME> interface
[<LAYER3-INTERFACE-NAME>|
          pppoe1|vlan <1-4094>|wwan1] [(address|interface|overload|pool
<NAT-POOL-NAME>)]

bridge vlan <1-4094>
```

Parameters

```
bridge nat source list <IP-ACCESS-LIST-NAME> interface
[<LAYER3-INTERFACE-NAME>|
pppoe1|vlan <1-4094>|wwan1] [(address|interface|overload|pool
<NAT-POOL-NAME>)]
```

nat	Configures *Network Address Translation* (NAT) parameters for an interface
source	Configures NAT source addresses
list <IP-ACCESS-LIST-NAME>	Associates an access list (describing local addresses) with the selected interface • <IP-ACCESS-LIST-NAME> – Specify access list name.
interface [<LAYER3-INTERFACE-NAME>| pppoe1| vlan <1-4094>| wwan1]	Selects one of the following as the primary interface: • <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 • overload – Enables use of one global address for multiple local addresses (terminates command) • pool <NAT-POOLNAME> – Configures the NAT pool used with the selected interface. Specify the NAT pool name.

```
bridge vlan <1-4095>
```

vlan <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
  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

Table 22 summarizes bridge VLAN configuration mode commands.

TABLE 22 Bridge-VLAN-Mode Commands

Command	Description	Reference
bridging-mode	Configures how packets on this VLAN are bridged	*page 7-414*
description	Configures VLAN bridge description	*page 7-415*
edge-vlan	Enables edge VLAN mode	*page 7-415*
firewall	Enables VLAN fire wall	*page 7-416*
ip	Configures IP components	*page 7-416*
l2-tunnel-broadcast-optimization	Enables broadcast optimization	*page 7-419*

TABLE 22 Bridge-VLAN-Mode Commands

Command	Description	Reference
no	Negates a command or reverts settings to their default	*page 7-419*
stateful-packet-inspection-12	Enables statedly packet inspection in the layer 2 fire wall	*page 7-422*
use	Uses pre configured access lists with this PF bridge policy	*page 7-423*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
do	Runs commands from the EXEC mode	*page 4-165*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes information to memory or terminal	*page 5-310*

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
bridging-mode [outlasted-tablecloths]
```

Parameters

```
bridging-mode [outlasted-tablecloths]
```

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
local	Bridges packets normally between local Ethernet ports and local radios (if any)
tunnel	Bridges packets between local Ethernet ports, local radios, and tunnels to other APs and wireless controllers

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 i gmp snooping
 ip i gmp snooping que ri er
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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
description <WORD>
```

Parameters

```
description <WORD>
```

description <WORD>	Configures a description for this VLAN bridge • <WORD> – Specify VLAN description.

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 i gmp snooping
 ip i gmp 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.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 • trust – Trusts ARP responses on the VLAN
dhcp trust	Configures the DHCP trust parameter • trust – Trusts DHCP responses on the VLAN

`ip igmp snooping {forward-unknown-multicast}`

ip	Configures the VLAN bridge IP parameters
igmp snooping	Configures *Internet Group Management Protocol* (IGMP) snooping parameter
forward-unknown-multicast	Optional. Enables forwarding of unknown multicast packets

`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
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.
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.

Usage Guidelines:

The IGMP protocol 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.

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. The feature is disabled by default.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
no
[bridging-mode|description|edge-vlan|firewall|ip|l2-tunnel-broadcast-optimiza
tion|
          stateful-packet-inspection-l2|use]

no
[bridging-mode|description|edge-vlan|firewall|l2-tunnel-broadcast-optimizatio
n|
          stateful-packet-inspection-l2]

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 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]
```

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 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 use [ap-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-12	Enables stateful packet inspection in the layer 2 firewall
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
do	Runs commands from the EXEC mode
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-12

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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.
run	Enables CDP sniffing and transmit globally
timer <5-900>	Specifies time between advertisements • <5-900> – Specify a value from 5 - 900 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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 (in a cluster) restarts When a wireless controller in the cluster fails, a secondary wireless controller or a set of wireless controllers manages the APs adopted by the failed wireless controller. When force-configured-state is set and a failed wireless controller restarts, APs that were adopted by it, and taken over by secondary wireless controllers, are moved back.
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
handle-stp	Configures *Spanning Tree Protocol* (STP) convergence handling
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.

```
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 mode as active or standby • active – Configures cluster mode as active • standby – Configures cluster mode as standby

```
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
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

Adds the wireless controller as part of a pool and group

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
controller [group|hello-interval|vlan|host]

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}
controller host [<IP>|<HOSTNAME>] {level [1|2]|pool <1-2> level [1|2]}
          {(ipsec-secure {gw})}
```

Parameters

```
controller [group <CONTROLLER-GROUP-NAME>|vlan <1-4094>]
```

controller	Configures the WLAN settings
group <CONTROLLER-GROUP-NAME>	Configures the wireless controller group • <CONTROLLER-GROUP-NAME> – Specify the wireless controller group name.
vlan <1-4094>	Configures the wireless controller VLAN • <1-4094> – Specify the VLAN ID from 1 - 4094.

```
controller hello-interval <1-120> adjacency-hold-time <2-600>
```

controller	Configures WLAN settings
hello-interval <1-120>	Configures the hello-interval in seconds. This is the interval between hello packets exchanged by AP and wireless controller. • <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 and AP is lost and 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 WLAN settings
host [<IP>|<HOSTNAME>]	Configures wireless controller's IP address or name • <IP> – Configures wireless controller's IP address • <HOSTNAME> – Configures wireless controller's name
level [1|2]	The following keywords are common to the 'IP' and 'hostname' parameters: Optional. After providing the wireless controller 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'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

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
```

Related Commands:

no	Disables or reverts settings to their default

critical-resource

Profile Config Commands

Monitors user configured IP addresses and logs their status

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 (publish even when “all” IP addresses are unreachable • any – Monitors any resource that is going down (publish even when “any” IP address 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) • 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’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 • any – Monitors any resource that is going down
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) • 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
 br300 00-15-70-63-4F-86 adopt
 br300 00-15-70-63-4F-97 adopt
 br300 00-A0-F8-CF-1E-DA adopt
 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.

Table 23 summarizes crypto configuration commands.

TABLE 23 Crypto-Config-Mode Commands

Command	Description	Reference
crypto	Defines a system-level local ID for ISAKMP negotiation	*page 7-432*
crypto-auto-ipsec-tunnel commands	Creates an auto IPSec VPN tunnel and changes the mode to auto-ipsec-secure mode for further configuration	*page 7-437*
crypto-ikev1-policy commands	Configures crypto IKEv1/IKEv2 policy parameters	*page 7-440*
crypto-ikev1-peer commands	Configures IKEv1 peer parameters	*page 7-445*
crypto-map commands	Configures crypto map parameters	*page 7-450*

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
crypto [auto-ipsec-secure|ikev1|ikev2|ipsec|load-management|map|pki|
       plain-text-deny-acl-scope]

crypto [auto-ipsec-secure|load-management]

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|include-alg-rules|security-association|transform-set]
crypto ipsec [df-bit [clear|copy|set]|include-alg-rules]
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]
```

Parameters

```
crypto [auto-ipsec-secure|load-management]
```

auto-ipsec-secure	Configures the Auto IPSec Secure parameter settings. For Auto IPSec tunnel configuration commands, see *crypto-auto-ipsec-tunnel commands*.
load-management	Configures load management for platforms using software cryptography

```
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-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-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]|include-alg-rules]
```

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
include-alg-rules	Includes ALG rules in IPSEC ACLs

```
crypto ipsec security-association lifetime [kilobytes <500-2147483646>|
seconds <120-86400>]
```

ipsec	Configures the *Internet Protocol Security* (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 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

Usage Guidelines:

If no peer IP address is configured, the manual crypto map is not valid and not complete. A peer IP address is required for manual crypto maps. To change the peer IP address, the no set peer command must be issued first, then the new peer IP address can be configured.

A peer address can be deleted with a wrong ISAKMP value. Crypto currently matches only the IP address when a no command is issued.

```
rfs7000-37FABE(config-profile-default-rfs7000)#crypto isakmp key 12345678
address 4.4.4.4
```

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#crypto ipsec transform-set
tpsec-tag1 ah-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
  bridging-mode isolated-tunnel
  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 cookie-challenge-threshold 1
 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 plain-text-deny-acl-scope interface
 interface me1
--More--
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)#crypto ikev2 remote-vpn

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)#

rfs7000-37FABE(config-profile-default-rfs7000)#crypto map map1 12 ipsec-isakmp
dynamic
```

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.

```
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
  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)#
```

Table 24 summarizes the crypto IPSec auto tunnel commands.

TABLE 24 IPSec-Auto-Tunnel Commands

Command	Description	Reference
groupid	Specifies the identity string used for IKE authentication	*page 7-438*
remotegw	Defines the IKE version used for an auto IPSec tunnel using secure gateways	*page 7-439*
no	Negates a command or sets its default	*page 7-439*

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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.
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

NOTE
Only one group ID is supported on the wireless controller. All APs and wireless controllers must use the same group ID.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-crypto-auto-ipsec-secure)#group
id
 exampleutions@123 rsa

rfs7000-37FABE(config-profile-default-rfs7000-crypto-auto-ipsec-secure)#show
context
 crypto auto-ipsec-secure
  groupid exampleutions@123 rsa
rfs7000-37FABE(config-profile-default-rfs7000-crypto-auto-ipsec-secure)#
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
remotegw ike-version [ikev1-aggr|ikev1-main|ikev2]
```

Parameters

```
remotegw ike-version [ikev1-aggr|ikev1-main|ikev2]
```

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

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-crypto-auto-ipsec-secure)#remot
egw-ike-version ikev2
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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
no groupid
```

Parameters

```
no groupid
```

groupid	Removes local/remote identity for auto IPSec IKE

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 exampleutions@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)#
```

crypto-ikev1-policy commands

crypto

Defines crypto-IKEv1/IKEv2 commands in detail

Use the (config) instance to configure IKEv1 policy configuration commands. To navigate to the IKEv1 policy instance, use the following commands:

```
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)#
```

Table 25 summarizes crypto IKEV1 commands.

TABLE 25 Crypto-IKEV1-Policy Commands

Command	Description	Reference
dpd-keepalive	Sets *Dead Peer Detection* (DPD) keep alive packet interval	*page 7-441*
dpd-retries	Sets the maximum number of attempts for sending DPD keep alive packets	*page 7-441*
isakmp-proposal	Configures ISAKMP proposals	*page 7-442*

TABLE 25 Crypto-IKEV1-Policy Commands

Command	Description	Reference
lifetime	Specifies how long an IKE SA is valid before it expires	*page 7-443*
mode	Sets the mode of the tunnels	*page 7-443*
no	Negates a command or sets its default	*page 7-444*

dpd-keepalive

crypto-ikev1-policy commands

Sets the *Dead Peer Detection* (DPD) keep-alive packet interval

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
dpd-keepalive <10-3600>
```

Parameters

```
dpd-keepalive <10-3600>
```

<10-3600>	Specifies the interval, in seconds, between successive DPD keep alive packets. Specify the time from 10 - 3600 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-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 peer is declared dead.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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-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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 *Advanced Encryption Standard* (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-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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 60 - 86400 seconds. • <60-86400> – Specify a value from 60 -86400 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-policy commands

Configures the IPSec mode of operation

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

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-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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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
isakmp-proposal	Removes the configured ISAKMP proposal
lifetime	Resets the ISAKMP security association lifetime
mode	Resets the tunnelling mode to default (main mode)

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-peer commands

crypto

Use the (config) instance to configure IKEv1 peer configuration commands. To navigate to the IKEv1 peer instance, use the following commands:

```
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 credentails
  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)#
```

Table 26 summarizes cyrpto IPSec peer configuration commands.

TABLE 26 Crypto-Peer-Mode Commands

Command	Description	Reference
authentication	Configures a peer's authentication mode and credentials	*page 7-446*
ip	Configures the peer's IP address	*page 7-447*
localid	Configures a peer's local identity details	*page 7-447*
remoteid	Configures a remote peer's identity details	*page 7-448*
use	Uses IKEv1 ISAKMP policy configuration settings	*page 7-449*
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 7-449*

authentication

crypto-ikev1-peer commands

Configures 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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 *Rivest-Shamir-Adleman* (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)#
```

ip

crypto-ikev1-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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 *Fully Qualified Domain Name* (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)#
```

localid

crypto-ikev1-peer commands

Sets a peer's local identity credentials

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
localid [address|dn|email|fqdn|string]
localid [address <IP>|dn <WORD>|email <WORD>|fqdn <WORD>|string <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.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-tespeer)#localid
email bob@example.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@example.com
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#
```

remoteid

crypto-ikev1-peer commands

Configures a peer's remote identity credentials

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 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@example.com
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#
```

use

crypto-ikev1-peer commands

Uses IKEv1 ISAKMP policy configuration settings

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
use ikev1-policy <IKEV1-POLICY-NAME>
```

Parameters

```
use ikev1-policy <IKEV1-POLICY-NAME>
```

use ikev1-policy <IKEV1-POLICY-NAME>	Specify the IKEv1 ISAKMP 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-tespeer)#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@example.com
  use ikev1-policy test-ikev1policy
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#
```

no

crypto-ikev1-peer commands

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.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
no [authentication|ip|localid|remoteid|use]
```

Parameters

```
no [authentication|ip|localid|remoteid|use]
```

authentication	Removes a peer's authentication credentials
ip	Removes a peer's IP address / FQDN
localid	Removes a peer's local identity details
remoteid	Removes a peer's remote identity details
use	Resets the IKEv1 ISAKMP policy settings

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@example.com
  use ikev1-policy test-ikev1policy
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#

rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-tespeer)#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)#
```

crypto-map 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).

Use the (config) instance to configure crypto map configuration commands. To navigate to the config-map instance, use the following commands:

```
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)#
```

Table 27 summarizes Crypto map configuration mode commands.

TABLE 27 Crypto-Map-Mode Commands

Command	Description	Reference
local-endpoint-ip	Uses the configured IP as local tunnel endpoint address, instead of the interface IP (Advanced Configuration)	*page 7-451*
mode	Sets the tunnel mode	*page 7-452*
peer	Sets the peer device's IP address	*page 7-452*
security-association	Defines the lifetime (in kilobytes and/or seconds) of IPSec SAs created by a crypto map	*page 7-453*
session-key	Defines encryption and authentication keys for a crypto map	*page 7-453*
use	Uses the configured IP access list	*page 7-455*
no	Negates a command or sets its default	*page 7-456*

local-endpoint-ip

crypto-map commands

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 commands

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 commands

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 commands

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 commands

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 71XX Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 *Security Parameter Index* (SPI) for the security association from 256 - 4294967295 The SPI (in combination with the destination IP address and security protoco) 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

```
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 Payloads* (ESP) 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|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 commands

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 commands

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 tunnelliing 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)#
```

dot1x

Profile Config Commands

Configures 802.1x standard authentication controls

Supported in the following platforms:

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

`dot1x guest-vlan supplicant`

system-auth-control	Configures guest VLAN and supplicant behavior
supplicant	Allows 802.1x capable supplicant to enter guest VLAN

`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.

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
 br300 00-15-70-63-4F-86 adopt
 br300 00-15-70-63-4F-97 adopt
 br300 00-A0-F8-CF-1E-DA adopt
 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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
dscp-mapping <WORD> priority <0-7>
```

Parameters

```
dscp-mapping <word> priority <0-7>
```

<WORD>	Specifies a 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
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
email-notification [host <IP>|recipient <RECIPIENT-EMAIL>]

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 • <RECIPIENT-EMAIL> – Specify the recipient's e-mail address.

```
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.
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.
password [2 <WORD>|<WORD>]	Configures the SMTP server password • 2 <WORD> – Configures an encrypted password • <WORD> – Specify the password.

```
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@example.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@example.com
 service pm sys-restart
```

Related Commands:

no	Disables or reverts settings to their default

enforce-version

Profile Config Commands

Checks device firmware versions before attempting connection

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
enforce-version [adoption|cluster] [full|major|none|strict]
```

Parameters

```
enforce-version [adoption|cluster] [full|major|none|strict]
```

adoption	Verifies firmware versions before adopting
cluster	Verifies firmware versions before clustering
full	Allows adoption or clustering when firmware versions exactly match
major	Allows adoption or clustering when major and minor versions exactly match
none	Allows adoption or clustering between any firmware versions
strict	Allows adoption or clustering only when firmware versions exactly match

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
  ip igmp snooping
  ip igmp snooping querier
 autoinstall configuration
 ....................................................
 interface pppoe1
 use firewall-policy default
 br300 00-15-70-63-4F-86 adopt
 br300 00-15-70-63-4F-97 adopt
 br300 00-A0-F8-CF-1E-DA adopt
 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

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
events [forward on|on]
```

Parameters

```
event [forward on|on]
```

forward on	Forwards system event messages to the wireless controller or cluster members • on – Enables forwarding of system events
on	Generates system events

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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@example.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@example.com
br300 00-15-70-63-4F-86 adopt
br300 00-15-70-63-4F-97 adopt
br300 00-A0-F8-CF-1E-DA adopt
service pm sys-restart
router ospf
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Disables export of startup.log file

interface

Profile Config Commands

Table 28 summarizes interface configuration commands.

TABLE 28 Interface-Config-Mode Commands

Command	Description	Reference
interface	Selects an interface to configure	*page 7-463*
interface-config-instance	Summarizes Ethernet interface (associated with the wireless controller) configuration commands	*page 7-465*
interface-vlan-instance	Summarizes VLAN interface configuration commands	*page 7-480*
interface-radio-instance	Summarizes radio interface configuration commands (applicable to access point profiles)	*page 7-488*

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
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]
```

Parameters

```
interface [<INTERFACE-NAME>|fe <1-4>|ge <1-8>|me1|port-channel <1-4>|radio
[1|2|3]|
up1|vlan <1-4094>|wwan1|xge <1-2>]
```

<INTERFACE-NAME>	Defines the interface name
fe <1-4>	Selects a FastEthernet interface • <1-4> – Specify the interface index from 1 - 4.
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
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
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
xge <1-2>	Selects a TenGigabitEthernet interface • <1-2> – Specify the interface index from 1 - 2.

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)#
```

Related Commands:

no	Removes the selected interface

interface-config-instance

interface

Use the config-profile-default-rfs7000 instance to configure the Ethernet, VLAN and tunnel associated with the wireless controller.

To switch to this mode, use the following command:

```
rfs7000-37FABE(config-profile-default-rfs7000)#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 <1-2>]
rfs7000-37FABE(config-profile-default-rfs7000)# ge 1

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
  no             Negate a command or set its defaults
  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)#
```

Table 29 summarizes the interface configuration commands.

TABLE 29 Interface-Config Commands

Command	Description	Reference
cdp	Enables *Cisco Discovery Protocol* (CDP) on ports	*page 7-466*
channel-group	Configures channel group commands	*page 7-467*
description	Creates an interface specific description	*page 7-467*
dot1x	Configures 802.1X authentication settings	*page 7-468*
duplex	Specifies the duplex mode for the interface	*page 7-470*
ip	Sets the IP address for the assigned Fast Ethernet interface (ME) and VLAN interface	*page 7-470*
lldp	Configures *Link Local Discovery Protocol* (LLDP)	*page 7-471*
no	Negates a command or sets its defaults	*page 7-472*
qos	Enables QoS	*page 7-473*
shutdown	Disables the selected interface	*page 7-474*
spanning-tree	Configures spanning tree parameters	*page 7-474*
speed	Specifies the speed of a FastEthernet or GigabitEthernet port	*page 7-476*
switchport	Sets interface switching mode characteristics	*page 7-477*
use	Defines the settings to use with this command	*page 7-479*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
do	Runs commands from the EXEC mode	*page 4-165*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes information to the memory or terminal	*page 5-310*

cdp

interface-config-instance

Enables *Cisco Discovery Protocol* (CDP) on wireless controller ports

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
cdp [transmit|receive]
```

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 wireless controller 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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
description [<LINE>|<WORD>]
```

Parameters

```
description [<LINE>|<WORD>]
```

[<LINE>|<WORD>]	Defines an interface description

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

interface-config-instance

Configures 802.1X authentication settings

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
dot1x [authenticator|supplicant]

dot1x authenticator [guest-vlan|host-mode|max-reauth-req|max-req|
port-control|
          reauthenticate|timeout]
```

```
dot1x authenticator [guest-val <1-4094>|host mode [multi-host|single-host]|
          max-reauth <1-10>|max-req <1-10>|port-control
[auto|force-authorized|
          force-unauthorized]|reauthenticate|timeout [quiet-period|
reauth-period]]

dot1x supplicant username <USERNAME> password [0 <WORD>|2 <WORD>|<WORD>]
```

Parameters

```
dot1x authenticator [guest-vlan <1-4094>|host mode [multi-host|single-host]|
max-reauth <1-10>|max-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. 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
max-reauth <1-10>	Configures maximum number of reauthorization retries for the supplicant • <1-10> – Specify a value from 1 -10.
max-req <1-10>	Configures maximum number of retries to RADIUS • <1-10> – Specify a value from 1 -10.
port-control [auto|force-authorized| force-unauthorized]	Configures port control state • auto – Configures auto port state • force-authorized – Configures authorized port state • force-unauthorized – Configures unauthorized port state
reauthenticate	Enables or disables re-authentication for this port
timeout [quiet-period| reauth-period]	Configures timeout settings for this interface • quiet-period – Configures the quiet period timeout • reauth-period – Configures the time after which re-authentication is initiated

```
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. 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

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#dot1x supplicant
username Bob password 0 exampleutions@123

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#show context
 interface ge1
  description This\ is\ GigabitEthernet\ interface\ for\ Royal\ King
  dot1x supplicant username Bob password 0 exampleutions@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	Disables or reverts interface settings to their default

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 exampleutions@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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 exampleutions@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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
no
[cdp|channel-group|description|dot1x|duplex|ip|lldp|qos|shutdown|spanning-tre
e|
          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 *Cisco Discovery Protocol* (CDP) on ports
channel-group	Configures channel group commands
description	Creates an interface specific description

dot1x	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 *Link Local Discovery Protocol* (LLDP)
no	Negates a command or reverts to defaults
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

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 exampleutions@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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 [disbale|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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 exampleutions@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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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. 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 exampleutions@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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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)#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 exampleutions@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-vlan-instance

interface

Use the config-profile-default-rfs7000 mode to configure Ethernet, VLAN and tunnel settings.

To switch to this mode, use the following commands:

```
rfs7000-37FABE(config-profile-default-rfs7000)#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]
rfs7000-37FABE(config-profile-default-rfs7000)#interface vlan 8
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#
```

Table 30 summarizes interface VLAN configuration commands.

TABLE 30 Interface-VLAN-Config-Mode Commands

Commands	Description	Reference
crypto	Defines the encryption module	*page 7-481*
description	Defines the VLAN interface description	*page 7-482*
dhcp-relay-incoming	Allows an onboard DHCP server to respond to relayed DHCP packets on this interface	*page 7-482*
ip	Configures *Internet Protocol* (IP) config commands	*page 7-483*

TABLE 30 Interface-VLAN-Config-Mode Commands

Commands	Description	Reference
no	Negates a command or sets its default	*page 7-485*
shutdown	Shuts down an interface	*page 7-487*
use	Defines the settings used with this command	*page 7-488*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
do	Runs commands from the EXEC mode	*page 4-165*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes information to memory or terminal	*page 5-310*

crypto

interface-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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
crypto map <CRYPTO-MAP-NAME>
```

Parameters

```
crypto map <CRYPTO-MAP-NAME>
```

map <CRYPTO-MAP-NAME>	Attaches a crypto map to the VLAN interface • <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-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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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-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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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-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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 *open shortest path first* (OSPF) authentication scheme. Options are message-digest, null, and simple-password.
message-digest	Configures *message digest* (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-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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
no [crypto|description|dhcp-relay-incoming|ip|shut-down|use]

no [crypto map|description|dhcp-relay-incoming|shut-down|use
<IP-ACCESS-LIST-NAME> in]

no ip [address|dhcp|helper-address|nat]

no ip [helper-address <IP>|nat]
no ip address [<IP/M> {secondary}|dhcp|zerconf {secondary}]
```

```
no ip dhcp client request options all
```

Parameters

```
no [crypto map|description|dhcp-relay-incoming|shut-down|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 shut-down	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	Disables 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	Disables 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
```

ip address	Disables 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

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 *Internet Protocol* (IP) config commands
shutdown	Disables an interface
use	Defines the settings used with this command

shutdown

interface-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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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-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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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-radio-instance

interface

This section documents radio interface configuration parameters common to all access point profiles.
To enter the *AP profile* > *radio interface* context, use the following commands:

rfs7000-37FABE(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
  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-share-mode         Configure the radio-share mode of operation for
                           this radio
  rate-selection           Default or Opportunistic rate relection
  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
txbf                            Configure Transmit Beamforming (TxBF) parameters
                                (DEMO FEATURE)
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)#
```

Table 31 summarizes interface radio interface configuration commands.

TABLE 31 Interface-Radio-Config-Mode Commands

Commands	Description	Reference
aeroscout	Enables Aeroscout Multicast packet forwarding	*page 7-491*
aggregation	Configures 802.11n aggregation parameters	*page 7-492*
airtime-fairness	Enables fair access for clients based on airtime usage	*page 7-494*
antenna-diversity	Transmits antenna diversity for non-11n transmit rates	*page 7-494*
antenna-downtilt	Enables *Advanced Element Panel Technology* (ADEPT) antenna mode	*page 7-495*
antenna-gain	Specifies the antenna gain for the selected radio	*page 7-496*
antenna-mode	Configures the radio antenna mode	*page 7-496*
beacon	Configures beacon parameters	*page 7-497*
channel	Configures a radio's channel of operation	*page 7-498*
data-rates	Specifies the 802.11 rates supported on a radio	*page 7-499*
description	Configures the selected radio's description	*page 7-502*
dfs-rehome	Reverts to configured home channel once *Dynamic Frequency Selection* (DFS) evacuation period expires	*page 7-503*
dynamic-chain-selection	Enables automatic antenna mode selection	*page 7-503*
ekahau	Enables Ekahau multicast packet forwarding	*page 7-504*
extended-range	Configures extended range	*page 7-505*
guard-interval	Configures the 802.11n guard interval	*page 7-506*
lock-rf-mode	Retains user configured RF mode settings for the selected radio	*page 7-507*
max-clients	Configures the maximum number of wireless clients allowed to associate with this radio	*page 7-508*
mesh	Configures radio mesh parameters	*page 7-509*
meshpoint	Maps an existing meshpoint to this radio interface	*page 7-510*

TABLE 31 Interface-Radio-Config-Mode Commands

Commands	Description	Reference
no	Negates or resets radio interface settings configures on a profile or a device	*page 7-510*
non-unicast	Configures the handling of non unicast frames on this radio	*page 7-513*
off-channel-scan	Enables selected radio's off channel scanning parameters	*page 7-515*
placement	Defines selected radio's deployment location	*page 7-517*
power	Configures the transmit power on this radio	*page 7-518*
preamble-short	Enables the use of short preamble on this radio	*page 7-519*
probe-response	Configures transmission parameters for probe response frames	*page 7-520*
radio-share-mode	Configures the mode of operation, for this radio, as radio-share	*page 7-520*
rate-selection	Sets the rate selection method to standard or opportunistic	*page 7-521*
rf-mode	Configures the radio's RF mode	*page 7-522*
rifs	Configures *Reduced Interframe Spacing* (RIFS) parameters on this radio	*page 7-523*
rts-threshold	Configures the *Request to Send* (RTS) threshold value on this radio	*page 7-524*
shutdown	Terminates or shuts down selected radio interface	*page 7-525*
sniffer-redirect	Captures and redirects packets to an IP address running a packet capture/analysis tool	*page 7-526*
stbc	Configures radio's *Space Time Block Coding* (STBC) mode	*page 7-527*
use	Enables use of an association ACL policy and a radio QoS policy by selected radio interface	*page 7-527*
wireless-client	Configures wireless client parameters on selected radio	*page 7-529*
wlan	Enables a WLAN on selected radio	*page 7-530*

aeroscout

interface-radio-instance

Enables Aeroscout Multicast packet forwarding

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000

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	Resets default Aeroscout multicast MAC address

aggregation

interface-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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000

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 <0-65535>
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
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 • 65536 – Advertises a maximum of 65535 bytes

`aggregation ampdu max-aggr-size tx <0-65535>`

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 <0-65535>	Configures the limit of transmitted frames • <0-65535> – Sets the limit from 0 - 65536 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 • 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
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-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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000

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-radio-instance

Transmits antenna diversity for non-11n transmit rates

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000

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-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

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, Brocade Mobility RFS4000.

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-radio-instance

Configures the antenna gain for a selected radio. Antenna gain defines the ability of an antenna to convert power into radio waves and vice versa.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000

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

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-radio-instance

Configures the antenna mode (the number of transmit and receive antennas) on the radio

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000

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 receive
2*2	Uses antenna A and C for both transmit and receive
default	Uses default antenna settings

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-radio-instance

Configures radio beacon parameters. Beacons are packets sent by the access point to synchronize a wireless network.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000

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 *Delivery Traffic Indication Message* (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 • 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
  beacon dtim-period bss 4 2
  beacon dtim-period bss 5 2
  beacon dtim-period bss 6 2
  beacon dtim-period bss 7 2
  --More--
```

Related Commands:

no	Removes the configured beacon parameters

channel

interface-radio-instance

Configures a radio's channel of operation

Supported in the following platforms:

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

- Wireless Controllers — Brocade Mobility RFS4000

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) • 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--
```

Related Commands:

no	Resets a radio's channel of operation

data-rates

interface-radio-instance

Configures the 802.11 data rates on this radio

Supported in the following platforms:

- Access Points —, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000

Syntax:

```
data-rates [b-only|g-only|a-only|bg|bgn|gn|an|default|custom]

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|mcs0-7|mcs8-15|mcs16-23|
          mcs0-15|mcs8-23|mcs0-23|basic-1|basic-2|
basic-5.5|basic-6|basic-9|basic-11|
          basic-12|
basic-18|basic-24|basic-36|basic-48|basic-54|basic-mcs0-7]]
```

Parameters

```
data-rates [b-only|g-only|a-only|bg|bgn|gn|an|default]
```

b-only	Supports operation in the 11b only mode
g-only	Uses rates that support operation in the 11g mode only
a-only	Uses rates that support operation in the 11a mode only
bg	Uses rates that support both 11b and 11g wireless clients
bgn	Uses rates that support 11b, 11g and 11n wireless clients
gn	Uses rates that support 11g and 11n wireless clients
an	Uses rates that support 11a and 11n wireless clients
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|mcs0-7|mcs8-15|mcs16-23|
mcs0-15|mcs8-23|mcs0-23|basic-1|basic-2| basic-5.5|basic-6|basic-9|basic-11|
basic-12|basic-18|basic-24|basic-36|basic-48|basic-54|basic-mcs0-7]
```

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 • mcs0-7 – Modulation and Coding Scheme 0-7 • mcs8-15 – Modulation and Coding Scheme 8-15 • mcs16-23 – Modulation and Coding Scheme 16-23 • mcs0-15 – Modulation and Coding Scheme 0-15 • mcs8-23 – Modulation and Coding Scheme 8-23 • mcs0-23 – Modulation and Coding Scheme 0-232 • 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-mcs0-7 – Modulation and Coding Scheme 0-7 as a basic rate

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--
```

Related Commands:

no	Resets the 802.11 data rates on a radio

description

interface-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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000

Syntax:

```
description <WORD>
```

Parameters

```
description <WORD>
```

<WORD>	Defines a description for the selected radio

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--
```

Related Commands:

no	Removes a radio's description

dfs-rehome

interface-radio-instance

Reverts to configured home channel once *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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000

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-radio-instance

Enables automatic antenna mode selection (single antenna for non-11n transmit rates)

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000

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	Use the configured transmit antenna mode for all clients

ekahau

interface-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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000

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 *Tasman Sniffer Protocol* (TZSP) port on Ekahau engine from 0 - 65535
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--
```

Related Commands:

no	Uses default Ekahau multicast MAC address

extended-range

interface-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

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--
```

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-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.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000

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)

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--
```

Related Commands:

no	Resets the 802.11n guard interval to default (long: 800nSec)

lock-rf-mode

interface-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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000

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--
```

Related Commands:

no	Allows Smart RF to change a radio's RF mode settings

max-clients

interface-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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000

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.

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-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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000

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)
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
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)
preferred-peer <1-6> <MAC>	Configures a preferred peer device • <1-6> – Configures the priority at which the peer node will be added • <MAC> – Sets the MAC address of the preferred peer device (Ethernet MAC of either an AP or a wireless controller 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

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--
```

Related Commands:

no	Disables mesh mode operation of the selected radio

meshpoint

interface-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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000

Syntax:

```
mesh <MESHPOINT-NAME> {bss <1-16>}
```

Parameters

```
mesh <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-br71xxTest-if-radio1)#meshpoint test bss 7
rfs7000-37FABE(config-profile-br71xxTest-if-radio1)#show context
 interface radio1
  meshpoint test bss 7
rfs7000-37FABE(config-profile-br71xxTest-radio1)#
```

Related Commands:

no	Disables meshpoint on the selected radio

no

interface-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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000

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-br71xxTest-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
  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)
  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-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 (2347)
  shutdown                    Re-enable the selected interface
  sniffer-redirect            Disable capture and redirection of packets
  stbc                        Configure Space-Time Block Coding (STBC) parameters
  txbf                        Configure Transmit Beamforming (txbf) 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-br71xxTest-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-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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000

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.
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-radio-instance

Enables selected radio's off channel scanning parameters

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000

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.
scan-interval <2-100>	Optional. Configures the scan interval in dtims • <2-100> – Specify a value from 2 - 100.

`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 *TaZmen Sniffer Protocol* (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--
```

Related Commands:

no	Disables radio off channel scanning

placement

interface-radio-instance

Defines the location where the radio is deployed

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000

Syntax:

```
placement [indoor|outdoor]
```

Parameters

```
placement [indoor|outdoor]
```

indoor	Radio is deployed indoors (uses indoor regulatory rules)
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--
```

Related Commands:

no	Resets a radio's deployment location

power

interface-radio-instance

Configures a radio's transmit power

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000

Syntax:

```
power [<1-27>|smart]
```

Parameters

```
power [<1-27>|smart]
```

power	Configures a radio's transmit power
<1-27>	Transmits power in dBm (actual power could be lower based on regulatory restrictions)
smart	Smart RF determines the optimum power

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--
```

Related Commands:

no	Resets a radio's transmit power

preamble-short

interface-radio-instance

Enables short preamble on this radio

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000

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--
```

Related Commands:

no	Disables the use of short preamble on a radio

probe-response

interface-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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000

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

```
probe-response rate [follow-probe-request|highest-basic|lowest-basic]
```

probe-response	Configures transmission parameters for probe response frames
rate	Configures the data rates for transmitted probe responses
follow-probe-request	Transmits probe responses at the same rate as the received request
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-share-mode

interface-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 71XX Access Point

- Wireless Controllers — Brocade Mobility RFS4000

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-radio-instance

Sets the rate selection method to standard or opportunistic

NOTE
This feature is not supported on Brocade Mobility RFS4000 wireless controller.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 71XX 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)

rf-mode

interface-radio-instance

Configures the radio's RF mode of operation

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000

Syntax:

```
rf-mode [2.4GHz-wlan|4.9GHz-wlan|5GHz-wlan|sensor]
```

Parameters

```
rf-mode [2.4GHz-wlan|4.9GHz-wlan|5GHz-wlan|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
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
  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--
```

Related Commands:

no	Resets the radio's RF mode of operation

rifs

interface-radio-instance

Configures *Reduced Interframe Spacing* (RIFS) parameters on this radio

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000

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
rx-only	Supports RIFS possession only

tx-only	Supports RIFS transmission only
tx-rx	Supports both RIFS transmission and possession

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--
```

Related Commands:

no	Disables radio's RIFS parameters

rts-threshold

interface-radio-instance

Configures the *Request to Send* (RTS) threshold value on this radio

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000

Syntax:

```
rts-threshold <1-2347>
```

Parameters

```
rts-threshold <1-2347>
```

<1-2347>	Specify the RTS threshold value from 1- 2347 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
  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--
```

Related Commands:

no	Resets a radio's RTS threshold to its default (2347)

shutdown

interface-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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000

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-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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000

Syntax:

```
sniffer-redirect [omnipeek|tzsp] <IP> channel [1|1+|10|10-|100--------165]
```

Parameters

```
sniffer-redirect [omnipeek|tzsp] <IP> channel [1|1+|10|10---------165]
```

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
[1|1+|10|10-|100|---------165]	Specify the channel to capture packets • 1 – Channel 1 in 20 MHz • 1+ – Channel 1 as primary, channel 5 as extension • 10 – Channel 10 in 20 MHz • 10- – Channel 10 as primary, channel 6 as extension • 100 – Channel 100 in 20 MHz

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--
```

Related Commands:

no	Disables packet capture and redirection

stbc

interface-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 6511 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-radio-instance

Enables an association ACL policy and a radio QoS policy for this radio interface

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000

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.
radio-qos-policy	Uses a specified radio QoS policy with this radio interface • <RADIO-QoS-POLICY-NAME> – Specify the radio QoS policy name

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
  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
--More--
```

Related Commands:

no	Dissociates the specified association ACL policy and radio QoS policy

wireless-client

interface-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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000

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. Advertises in the Symbol/Brocade information element (176) • symbol-ie – Advertises in the Symbol/Brocade information element (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--
```

Related Commands:

no	Resets the transmit power indicated to wireless clients

wlan

interface-radio-instance

Enables a WLAN on this radio

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000

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 WLAN as the primary WLAN when multiple WLANs exist on the BSS • primary – Optional. Uses the 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
```

```
  non-unicast tx-rate bss 7 highest-basic
  non-unicast tx-rate bss 8 highest-basic
  non-unicast tx-rate bss 9 highest-basic
--More--
```

Related Commands:

no	Disables a WLAN on a radio

ip

Profile Config Commands

Table 32 summarizes NAT pool configuration commands.

TABLE 32 NAT-Pool-Config-Mode Commands

Command	Description	Reference
ip	Configures IP components, such as default gateway, DHCP, *Domain Name Service* (DNS) server forwarding, name server, domain name, routing standards etc.	*page 7-531*
nat-pool-config-instance	Invokes *Network Address Translation* (NAT) pool configuration parameters	*page 7-536*

ip

ip

Configures IP components, such as default gateway, DHCP, *Domain Name Service* (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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 [include-alg-rules|inside|outside|pool]

ip nat [include|alg-rules|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> <NATTED-IP>

ip nat [insdie|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 *Dynamic Host Control Protocol* (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	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 [include-alg-rules|pool <NAT-POOL-NAME>]`

nat	Configures the *Network Address Translation* (NAT) parameters
include-alg-rules	Includes the *Application Layer Gateway* (ALG) rules in the NAT ACL
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> <NATTED-IP>
```

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> <NATTED-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. • <NATTED-IP> – Specify the natted IP address to map.

```
ip nat [insdie|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 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
 br300 00-15-70-63-4F-86 adopt
 br300 00-15-70-63-4F-97 adopt
 br300 00-A0-F8-CF-1E-DA adopt
 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-default-rfs7000 instance to configure *Network Address Translation* (NAT) pool parameters.

```
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)
```

Table 33 summarizes NAT pool configuration commands.

TABLE 33 NAT-Pool Commands

Command	Description	Reference
address	Configures NAT pool addresses	*page 7-537*
no	Negates a command or sets its default	*page 7-538*
clrscr	Clears the display screen	*page 5-275*

TABLE 33 NAT-Pool Commands

Command	Description	Reference
commit	Commits (saves) changes made in the current session	*page 5-276*
do	Runs commands from the EXEC mode	*page 4-165*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes information to memory or terminal	*page 5-310*

address

nat-pool-config-instance

Configures NAT pool IP addresses

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 *Layer 2 Tunnel Protocol* (L2TP) protocol for tunneling layer 2 payloads using VPNs

Supported in the following platforms:

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

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 • <HOSTNAME> – Specify the L2TPV3 specific host name.
inter-tunnel-bridging	Enables inter tunnel bridging of packets
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, on this device, running the L2TPV3 service • <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
 ..............................................
 vrrp 1 timers advertise 1
 vrrp 1 preempt
 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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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--
```

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 71XX Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
led
```

Parameters

None

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#led
% Error: led configuration not available for this platform
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Disables or reverts settings to their default

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
legacy-auto-update [br650|br71xx image <FILE>]
```

Parameters

```
legacy-auto-update [br650|br71xx image <FILE>]
```

legacy-auto-update	Updates an Brocade Mobility 650 Access Point or Brocade Mobility 71XX Access Point legacy access point firmware
br650	Auto updates legacy Brocade Mobility 650 Access Point firmware
br71xx image <FILE>	Auto updates legacy Brocade Mobility 71XX Access Point firmware • image – Sets the path to the firmware image • <FILE> – Specify the path and filename in the flash:/ap.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 *Link Layer Discovery Protocol* (LLDP) settings

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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--
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
load-balancing [advanced-params|balance-ap-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|ap-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|ap-load]
[client-weightage|
          throughput-   weightage] <0-100>
load-balancing advanced-params equality-margin [2.4GHz|5GHz|ap|band] <0-100>
load-balancing advanced-params hiwater-threshold
[ap|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-ap-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|ap-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
ap-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|ap|band] <0-100>`

advanced-params	Configures advanced load balancing parameters
equality-margin [2.4GHz|5GHz|ap|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 • ap – 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 [ap|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
[ap|channel-2.4GHz| channel-5GHz] <0-100>	Select one of the following options: • ap – 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 0 - 100 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 0 - 100 dBm.

	`load-balancing [balance-ap-loads|balance-band-loads| balance-channel-loads [2.4GHz|5GHz]]`
balance-ap-loads	Enables neighbor AP load balancing
balance-band-loads	Enables balancing of the total band load amongst neighbors
balance-channel-loads [2.4GHz|5GHz]	Enables the following: • 2.4GHz – Balances channel loads on 2.4 GHz band • 5GHz – Balances channel loads on 5.0 GHz band

	`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
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
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

	`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 ap 90

rfs7000-37FABE(config-profile-default-rfs7000)#load-balancing
balance-ap-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 ap 90
 load-balancing balance-ap-loads
--More--
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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|local16|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 • <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
[<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 • 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|local16|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
 br300 00-15-70-63-4F-86 adopt
 br300 00-15-70-63-4F-97 adopt
 br300 00-A0-F8-CF-1E-DA adopt
 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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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--
```

Related Commands:

no	Disables or reverts settings to their default

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
meshpoint-device <MESHPOINT-NAME>
```

Parameters

```
meshpoint-device <MESHPOINT-NAME>
```

meshpoint-device <MESHPOINT-NAME>	Configures meshpoint device parameters • <MESHPOINT-NAME> – Specify meshpoint name.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#meshpoint-device TestMeshpoint
% Error: Meshpoint device parameters cannot be changed for device [rfs7000]
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Removes a specified meshpoint

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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--
```

Related Commands:

no	Resets the meshpoint monitoring interval to default (30 seconds)

min-misconfiguration-recovery-time

Profile Config Commands

Configures the minimum connectivity verification time

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
mint [dis|level|link|mlcp|spf-latency|tunnel-across-extended-vlan|
          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-across-extended-vlan
]
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. 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-across-extended-vlan
```

tunnel-across-extended-vlan	Enables tunneling of MiNT packets across extended VLANs. When disabled, only non-MiNT packets are tunneled. This feature is disabled by default.

```
mint tunnel-controller-load-balancing level1
```

tunnel-controller-load-balancing level1	Configures load balancing of MiNT extended VLAN traffic across tunnels • level1 – Configures tunnel wireless controller load balancing 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--
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
misconfiguration-recovery-time <60-300>
```

Parameters

```
misconfiguration-recovery-time <60-300>
```

<60-300>	Sets the recovery time from 60 - 300 seconds (default is 180 seconds)

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
 br300 00-15-70-63-4F-86 adopt
 br300 00-15-70-63-4F-97 adopt
 br300 00-A0-F8-CF-1E-DA adopt
 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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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--
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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--
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
no [ap-upgrade|br300|arp|auto-learn-staging-config|autoinstall|
bridge|cdp|cluster|
          configuration-persistence|controller|critical-resource|
crypto|dot1x|dscp-mapping|
          email-notification|events|export|interface|ip|l2tpv3|
l3e-lite-table|led|
          legacy-auto-downgrade|legacy-auto-update|lldp|load-balancing|
logging|
          mac-address-table|memory-profile|meshpoint-device|
meshpoint-monitor-interval|
          min-misconfiguration-recovery-time|mint|
misconfiguration-recovery-time|noc|ntp|
          preferred-controller-group|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:

ap-upgrade	Enables automatic AP firmware upgrade
br300	Enables adoption of Brocade Mobility 300 Access Points
arp	Configures static address resolution protocol
auto-learn-staging-config	Enables network configuration device learning
autoinstall	Configures the autoinstall feature
bridge	Configures bridge specific commands
cdp	Enables *Cisco Discovery Protocol* (CDP) on a device
cluster	Configures a cluster name
configuration-persistence	Enables configuration persistence across reloads
controller	Configures a wireless controller
critical-resource	Monitors user configured IP addresses and logs their status
crypto	Configures crypto settings
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
events	Displays system event messages

export	Enables the export of the startup.log file after every boot
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
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
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
noc	Configures NOC settings
ntp	Configures an NTP server
preferred-controller-group	Specifies the wireless controller group preferred for adoption
preferred-tunnel-controller	Configures the tunnel wireless controller name
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
wep-shared-key-auth	Enables support for 802.11 WEP shared key authentication
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
do	Runs commands from the EXEC mode
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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 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
 br300 00-15-70-63-4F-86 adopt
 br300 00-15-70-63-4F-97 adopt
 br300 00-A0-F8-CF-1E-DA adopt
 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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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
 br300 00-15-70-63-4F-86 adopt
 br300 00-15-70-63-4F-97 adopt
 br300 00-A0-F8-CF-1E-DA adopt
 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.

Supported in the following platforms:

- Access Points — Brocade Mobility 71XX 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 af power option. The options are: • range – Configures the af power range mode. This mode provides higher power but fewer transmission (tx) chains. • throughput – Configures the af power throughput mode. This mode provides lower power but has more tx chains.
at-option [range|throughput]	Configures the at power option. The options are: • range – Configures the at power range mode. This mode provides higher power but fewer tx chains. • throughput – Configures the at power throughput mode. This mode provides lower power but has more tx chains.

`power-config mode [auto|3af]`

mode [auto|3af]	Configures the AP power mode • 3af – Forces an AP power up at the 3af power mode • auto – Sets the detection auto mode

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)#
```

preferred-controller-group

Profile Config Commands

Specifies the group preferred for adoption

Supported in the following platforms:

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

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
preferred-controller-group <WORD>
```

Parameters

```
preferred-controller-group <WORD>
```

<WORD>	Specify the name of the group preferred for adoption

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
 br300 00-15-70-63-4F-86 adopt
 br300 00-15-70-63-4F-97 adopt
 br300 00-A0-F8-CF-1E-DA adopt
 service pm sys-restart
 router ospf
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands:

no	Removes the preferred group configuration

preferred-tunnel-controller

Profile Config Commands

Configures the tunnel preferred by the system for tunneling extended VLAN traffic

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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--
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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
 br300 00-15-70-63-4F-86 adopt
 br300 00-15-70-63-4F-97 adopt
 br300 00-A0-F8-CF-1E-DA adopt
 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 *Chapter 25, Router-Mode Commands*.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
router ospf
```

Parameters

```
router ospf
```

ospf	Enables *Open Shortest Path First* (OSPF) settings. Changes configuration mode to router mode 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.

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)#
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 *bridge protocol data units* (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 with the same instance, VLAN mapping, revision number and region names define a unique region. Wireless Controllers 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's name

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
tunnel-controller <NAME>
```

Parameters

```
tunnel-controller <NAME>
```

tunnel-controller <NAME>	Configures the tunneled WLAN (extended VLAN) wireless controller's name • <NAME> – Specify a name.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#tunnel-controller testgroup
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax: Profiles Mode

```
use [advanced-wips-policy|auto-provisioning-policy|captive-portal|
dhcp-server-policy|
          event-system-policy|firewall-policy|management-policy|
radius-server-policy|
          role-policy|routing-policy]
```

Syntax: Device Mode

```
use [advanced-wips-policy|auto-provisioning-policy|captive-portal|
dhcp-server-policy|

          event-system-policy|firewall-policy|management-policy|profile|
radius-server-policy|

          rf-domain|role-policy|routing-policy|wips-policy]
```

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|dhcp-server-pol
icy|
event-system-policy|firewall-policy|management-policy|radius-server-policy|
role-policy|
routing-policy]
```

use	Associates the specified policies with this profile The policies specified 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.

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.
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.

ParametersDevice Mode

```
use [advanced-wips-policy|auto-provisioning-policy|captive-portal|
dhcp-server-policy|
event-system-policy|firewall-policy|management-policy|profile|
radius-server-policy|
rf-domain|role-policy|routing-policy|wips-policy]
```

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.
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.
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 <ROLE-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.

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--
```

Related Commands:

no	Disassociates a specified policy from this profile

vrrp

Profile Config Commands

Configures *Virtual Router Redundancy Protocol* (VRRP) group settings

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 group ID from 1- 255. Identifies the virtual router the packet is reporting on.
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 this VRRP group • <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 • <P-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 activate VRRP failover, it is essential all individual groups within a synchronized group have failover.

```
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 group ID from 1- 255. Identifies the virtual router the packet is reporting on.
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 criticial-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 on.
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
pppoel	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 on.
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 msec - 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)

Usage Guidelines:

The node that wins the election enters the MASTER state and owns the virtual IP addresses. The Master node performs the following functions:

- Responds to ARP requests.
- Forwards packets with a destination link layer MAC address equal to the virtual router MAC address.
- Does not accept 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.

The nodes that loose the election enter the BACKUP state and monitor the Master for any failures. In case of a failure, one of the Backup router becomes the Master and takes over the virtual IPs.

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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--
```

Related Commands:

no	Disable support for 802.11 WEP shared key authentication

Device Config Commands

Use the (config) instance to configure device specific parameters

To navigate to this instance, use the following commands:

```
rfs7000-37FABE(config)#br7131 00-04-96-4A-A7-08
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#?
Device Mode commands:
  ap-mobility                       Configure AP mobility
  ap-upgrade                        AP firmware upgrade
  br300                             Adopt/unadopt BR300 device to this
                                    profile/device
  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
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                          Add controller
country-code                        Configure the country of operation
critical-resource                   Critical Resource
crypto                              Encryption related commands
dhcp-redundancy                     Enable DHCP redundancy
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
events                              System event messages
export                              Export a file
floor                               Set name of a floor within a area where
                                    the system is located
hostname                            Set system's network name
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
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-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
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
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
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

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

Table 34 summarizes device mode commands.

TABLE 34 Device-Mode Commands

Command	Description	Reference
ap-mobility	Configures AP mobility (fixed or vehicle mounted)	*page 7-406*
ap-upgrade	Enables automatic up gradation of AP firmware	*page 7-406*
br300	Enables adoption of Brocade Mobility 300 Access Points by a profile or wireless controller	*page 7-407*
area	Sets the name of area where the system is deployed	*page 7-583*
arp	Configures ARP parameters	*page 7-408*

TABLE 34 Device-Mode Commands

Command	Description	Reference
auto-learn-staging-config	Enables the automatic recognition of devices pending adoption	*page 7-410*
autoinstall	Autoinstalls firmware image and configuration setup parameters	*page 7-410*
bridge	Configures Ethernet Bridging parameters	*page 7-411*
captive-portal	Configures captive portal advanced Web page upload on this profile	*page 7-424*
cdp	Operates CDP on the device	*page 7-424*
channel-list	Configures channel list advertised to wireless clients	*page 7-584*
cluster	Sets cluster configuration	*page 7-425*
configuration-persistence	Enables configuration persistence across reloads	*page 7-427*
contact	Sets contact information	*page 7-584*
controller	Configures a WLAN wireless controller	*page 7-428*
country-code	Configures wireless controller's country code	*page 7-585*
critical-resource	Monitors user configured IP addresses and logs their status	*page 7-430*
crypto	Configures crypto settings	*page 7-432*
dhcp-redundancy	Enables DHCP redundancy	*page 7-586*
dot1x	Configures 802.1x standard authentication controls	*page 7-457*
dscp-mapping	Configures IP *Differentiated Services Code Point* (DSCP) to 802.1p priority mapping for untagged frames	*page 7-458*
email-notification	Configures e-mail notification	*page 7-459*
enforce-version	Checks the device firmware version before attempting connection	*page 7-460*
events	Displays system event messages	*page 7-461*
export	Enables export of startup.log file after every boot	*page 7-462*
floor	Sets the building floor where the system is deployed	*page 7-587*
hostname	Sets a system's network name	*page 7-587*
interface	Selects an interface to configure	*page 7-463*
ip	Configures IP components	*page 7-531*
l2tpv3	Defines the *Layer 2 Tunnel Protocol* (L2TP) protocol for tunneling Layer 2 payloads using *Virtual Private Networks* (VPNs)	*page 7-538*
l3e-lite-table	Configures L3e Lite Table with this profile	*page 7-539*
layout-coordinates	Configures layout coordinates	*page 7-588*
led	Turns LEDs on or off	*page 7-540*
legacy-auto-downgrade	Enables legacy device firmware to auto downgrade	*page 7-541*
legacy-auto-update	Auto updates Brocade Mobility 650 Access Point and Brocade Mobility 71XX Access Point legacy device firmware	*page 7-541*
license	Adds a license for a device's features	*page 7-589*
lldp	Configures *Link Layer Discovery Protocol* (LLDP) settings for this profile	*page 7-542*
load-balancing	Configures load balancing parameters.	*page 7-543*

TABLE 34 Device-Mode Commands

Command	Description	Reference
location	Configures the location the system is deployed	*page 7-590*
logging	Enables message logging	*page 7-547*
mac-address-table	Configures the MAC address table	*page 7-549*
mac-name	Configures MAC name to name mappings	*page 7-590*
memory-profile	Configures memory profile used on the device	*page 7-550*
meshpoint-device	Configures meshpoint device parameters	*page 7-551*
meshpoint-monitor-interval	Configures meshpoint monitoring interval	*page 7-551*
min-misconfiguration-recovery-time	Configures the minimum wireless controller connectivity verification time	*page 7-552*
mint	Configures MiNT protocol commands	*page 7-553*
misconfiguration-recovery-time	Verifies wireless controller connectivity after a configuration is received	*page 7-556*
neighbor-inactivity-timeout	Configures a neighbor inactivity timeout	*page 7-557*
neighbor-info-interval	Configures the neighbor information exchange interval	*page 7-591*
no	Negates a command or resets values to their default settings	*page 7-558*
noc	Configures NOC settings	*page 7-561*
ntp	Configure the NTP server settings	*page 7-562*
override-wlan	Configures WLAN RF Domain level overrides	*page 7-595*
power-config	Configures power mode features	*page 7-563*
preferred-controller-group	Specifies the wireless controller group the system prefers for adoption	*page 7-564*
preferred-tunnel-controller	Configures the tunnel wireless controller preferred by the system for tunneling extended VLAN traffic	*page 7-565*
radius	Configures device-level RADIUS authentication parameters	*page 7-566*
remove-override	Removes device overrides	*page 7-596*
rf-domain-manager	Enables the RF Domain manager	*page 7-567*
router	Configures dynamic router protocol settings.	*page 7-568*
rsa-key	Assigns a RSA key to SSH	*page 7-598*
sensor-server	Configures an AirDefense sensor server	*page 7-599*
spanning-tree	Enables spanning tree commands	*page 7-569*
stats	Configures statistics settings	*page 7-600*
timezone	Configures wireless controller time zone settings	*page 7-601*
trustpoint	Assigns a trustpoint to a service	*page 7-602*
tunnel-controller	Configures the tunneled WLAN (extended-vlan) wireless controller's name	*page 7-571*
use	Defines the settings used with this command	*page 7-572*
vrrp	Configures *Virtual Router Redundancy Protocol* (VRRP) group settings	*page 7-574*

TABLE 34 Device-Mode Commands

Command	Description	Reference
wep-shared-key-auth	Enables support for 802.11 WEP shared key authentication	*page 7-577*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
do	Runs commands from the EXEC mode	*page 4-165*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes information to memory or terminal	*page 5-310*

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
area <AREA-NAME>
```

Parameters

```
area <AREA-NAME>
```

area <AREA-NAME>	Sets the area where the system is deployed

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 exampleutions

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 exampleutions
 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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 exampleutions
 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

dhcp-redundancy

Device Config Commands

Enables DHCP redundancy

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
dhcp-redundancy
```

Parameters

None

Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#dhcp-redundancy

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 exampleutions
 country-code us
 dhcp-redundancy
 channel-list 2.4GHz 1,2
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
floor <WORD>
```

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 exampleutions
 country-code us
 dhcp-redundancy
 channel-list 2.4GHz 1,2
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

Related Commands:

no	Removes configured device's location floor name

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
hostname <WORD>
```

Parameters

```
hostname <WORD>
```

hostname <WORD>	Sets the name of the managing wireless controller or access point. This name is displayed when accessed from any network.

Example

```
rrfs7000-37FABE(config-device-00-04-96-4A-A7-08)#hostname TechPubBR7131

The hostname has changed from 'br7131-4AA708' to 'TechPubBR7131'

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 TechPubBR7131
 area RMZEcospace
 floor 5thfloor
 contact exampleutions
 country-code us
 dhcp-redundancy
 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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 TechPubBR7131
 area RMZEcospace
 floor 5thfloor
 layout-coordinates 1.0 2.0
 contact exampleutions
 country-code us
 dhcp-redundancy
 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 for specific features

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
license <WORD> <LICENSE-KEY>
```

Parameters

```
license <WORD> <LICENSE-KEY>
```

<WORD>	Specify the feature name (AP/AAP/ADSEC/ADVANCED-WIPS/HOTSPOT-ANALYTICS) for which license is added
<LICENSE-KEY>	Specify the license key

Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#license ap aplicenseley@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 TechPubBR7131
 floor 5thfloor
 layout-coordinates 1.0 2.0
 license AP aplicenseley@1234 aplicensekey@123
 location Block3B
```

```
 no contact
 country-code us
 dhcp-redundancy
 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)#
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 TechPubBR7131
 area RMZEcospace
 floor 5thfloor
 layout-coordinates 1.0 2.0
 location Block3B
 contact exampleutions
 country-code us
 dhcp-redundancy
 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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 TechPubBR7131
 area RMZEcospace
 floor 5thfloor
 layout-coordinates 1.0 2.0
 location Block3B
 contact exampleutions
 country-code us
 dhcp-redundancy
 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 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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 TechPubBR7131
 area RMZEcospace
 floor 5thfloor
 layout-coordinates 1.0 2.0
 location Block3B
 contact exampleutions
 country-code us
 dhcp-redundancy
 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)#
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
no
[ap-mobility|ap-upgrade|br300|area|arp|auto-learn-staging-config|autoinstall|

bridge|cdp|channel-list|cluster|configuration-persistence|contact|controller|

country-code|critical-resource|crypto|dhcp-redundancy|dot1x|dscp-mapping|

email-notification|events|export|floor|hostname|interface|ip|l2tpv3|
          layout-coordinates|led|legacy-auto-downgrade|
legacy-auto-update|lldp|load-balancing|

location|logging|mac-address-table|mac-name|memory-profile|meshpoint-device|
          meshpoint-monitor-interval|min-misconfiguration-recovery-time|mint|
```

```
misconfiguration-recovery-time|noc|ntp|override-wlan|preferred-controller-gro
up|
          preferred-tunnel-controller|
radius|rf-domain-manager|router|rsa-key|sensor-server|
          spanning-tree|stats|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:

ap-mobility	Configures AP mobility (fixed or vehicle mounted)
ap-upgrade	Upgrades AP firmware
br300	Enables adoption of Brocade Mobility 300 Access Points by a profile
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
dhcp-redundancy	Enables DHCP redundancy
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

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
hostname	Sets a system's network name
interface	Selects an interface to configure
ip	Configures IP components
l2tpv3	Defines the L2TP protocol for tunneling layer 2 payloads using VPNs
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 *Link Layer Discovery Protocol* (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-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
stats	Configures statistics settings
timezone	Configures time zone settings
trustpoint	Assigns a trustpoint to a service
tunnel-controller	Configures the tunneled WLAN (extended-vlan) wireless controller's name
use	Defines the settings used by this feature
vrrp	Configures *Virtual Router Redundancy Protocol* (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
do	Runs commands from the EXEC mode
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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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. 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 TechPubBR7131
 floor 5thfloor
 layout-coordinates 1.0 2.0
 license AP aplicenseley@1234 aplicensekey@123
 location Block3B
 no contact
 country-code us
 dhcp-redundancy
 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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
remove-override <PARAMETERS>
```

Parameters

None

Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#remove-override ?
  all                          Remove all overrides for the device
  ap-upgrade                   AP firmware upgrade
  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
  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
  dhcp-redundancy              DHCP redundancy
  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
  events                       System event messages
  export                       Export a file
  firewall                     Enable/Disable firewall
  global                       Remove global overrides for the device but
                               keeps per-interface overrides
  interface                    Select an interface to configure
  ip                           Internet Protocol (IP)
  l2tpv3                       L2tpv3 protocol
  lldp                         Link Layer Discovery Protocol
  location                     The location
  logging                      Modify message logging facilities
  mac-address-table            MAC Address Table
  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
```

```
  stats                          Stats-window related configuration
  timezone                       The timezone
  tunnel-controller              Tunnel Controller group this controller belongs
                                 to
  use                            Set setting to use
  vrrp                           VRRP configuration

  service                        Service Commands

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 TechPubBR7131
 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
 dhcp-redundancy
 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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 TechPubBR7131
 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
 dhcp-redundancy
 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

stats

Device Config Commands

Configures settings for the display of system statistics

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
stats open-window <1-2> {sample-interval <5-86640>} {size <3-100>}
```

Parameters

```
stats open-window <1-2> {sample-interval <5-86640>} {size <3-100>}
```

open-window <1-2>	Opens a stats window to fetch trending data. Set the index from 1 - 2.
sample-interval <5-86640>	Optional. Sets the sample interval from 5 - 86640 seconds
size <3-100>	Optional. Sets the stats window size and number of samples collected

Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#stats open-window 2
sample-interval 77 size 10

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 TechPubBR7131
 floor 5thfloor
 layout-coordinates 1.0 2.0
 license AP aplicenseley@1234 aplicensekey@123
 rsa-key ssh rsa-key1
 location Block3B
 no contact
 stats open-window 2 sample-interval 77 size 10
 country-code us
 dhcp-redundancy
 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 statistics related settings

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 TechPubBR7131
 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
 dhcp-redundancy
 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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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>	Uses EAP to assign a trustpoint as a certificate authority for validating client certificates • <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 TechPubBR7131
 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
 dhcp-redundancy
 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

In this chapter

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) can also be utilized to provide user database information and user authentication data. Each WLAN can maintain 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:

```
RFSSwitch(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 35 summarizes AAA policy configuration commands.

TABLE 35 AAA-Policy-Config Commands

Command	Description	Reference
accounting	Configures accounting parameters	*page 8-605*
attribute	Configure RADIUS attributes in access and accounting requests	*page 8-608*
authentication	Configures authentication parameters	*page 8-609*
health-check	Configures health check parameters	*page 8-612*
mac-address-format	Configures the MAC address format	*page 8-613*
no	Negates a command or sets its default	*page 8-614*
proxy-attribute	Configures the RADIUS server's attribute behavior when proxying through the wireless controller or the RF Domain manager	*page 8-617*
server-pooling-mode	Defines the method for selecting a server from the pool of configured AAA servers	*page 8-618*
use	Defines the AAA command settings	*page 8-619*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
do	Runs commands from the EXEC mode	*page 4-165*

TABLE 35 AAA-Policy-Config Commands

Command	Description	Reference
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes information to memory or terminal	*page 5-310*

accounting

aaa-policy

Configures the server type and interval 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers – Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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-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.

	`accounting server preference [auth-server-host|auth-server-number|none]`
server	Configures an accounting server
preference	Configures the accounting server preference
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 referred to 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 referred to 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 retry timeouts • <50-200> – Specify a value from 50 - 200. A value of 100 indicates the interval between two consecutive retries is the same, irrespective of the number of retries. If the scaling factor value is less than 100, the time interval between two consecutive retires keeps reducing with subsequent retries. If this value is greater than 100, the time interval between two consecutive retries keeps increasing 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 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	Configures the *Network Access Identifier* (NAI)
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) • suffix – Matches the suffix of the username (For example, user1@DOMAIN, user2)@DOMAIN)
realm	Specifies the text matched against the username
<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, or wireless controller, where the client is associated
controller	Configures local RADIUS server settings

```
accounting server <1-6> proxy-mode
[none|through-controller|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 wireless controller configuring the device
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. Specified 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
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 brocade 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 brocade 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers – Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
attribute framed-mtu <100-1500>
```

Parameters

```
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.

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 brocade 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)#
```

Related Commands:

no	Resets values or disables commands

authentication

aaa-policy

Configures authentication parameters

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers – Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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-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 number of attempts to authenticate a wireless client • <1-10> – Specify a value from 1 - 10.
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.
retry-timeout-factor <50-200>	Configures the spacing between successive EAP retries • <50-200> – Specify a value from 50 - 200. A value of 100 indicates the interval between two consecutive retries is the same irrespective of the number of retries. If the scaling factor value is less than 100, the interval between two consecutive retires keeps reducing with subsequent retries. If this value is greater than 100, the interval between two consecutive retries keeps increasing with subsequent retries.
timeout <1-60>	Configures the interval, in seconds, between successive EAP-identity request retries 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.

`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 server's IP address or hostname
secret [0 <SECRET>|2 <SECRET>|<SECRET>]	Configures the RADIUS server 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 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	Configures the RADIUS authentication server <1-6> used as a *Network Access Control* (NAC) server for devices requiring NAC

	`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	Configures *Network Access Identifier* (NAI) RADIUS authentication
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 • <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-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-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-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 attempt. • A value greater than 100 indicates the interval between two consecutive retries increases with each successive retry attempt.

```
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.
attempts <1-10>	Optional. Indicates the number of retry attempts to make before giving up • <1-10> – Specify a value from 1 -10.

Example

```
rfs7000-37FABE(config-aaa-policy-test)#authentication server 5 host
172.16.10.10 secret brocade 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 brocade port 1009
 authentication server 5 timeout 10
 accounting server 2 host 172.16.10.10 secret 0 brocade 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers – Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 brocade port 1009
 authentication server 5 timeout 10
 accounting server 2 host 172.16.10.10 secret 0 brocade 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers – Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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
pair-colon	Configures the MAC address format as AA:BB:CC:DD:EE:FF
pair-hyphen	Configures the MAC address format as AA-BB-CC-DD-EE-FF (default setting)
quad-dot	Configures the MAC address 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
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

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 brocade port 1009
 authentication server 5 timeout 10
 accounting server 2 host 172.16.10.10 secret 0 brocade 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)#
```

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers – Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 framed-mtu
```

```
no authentication [eap|protocol|server]
no authentication eap wireless-client [attempts|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 preference

`no accounting server <1-6> {dscp|nai-routing|proxy-mode|retry-timeout-factor|timeout}`

no accounting server <1-6>	Resets the accounting server preference for the server specified by index <1-6>
dscp	Optional. Resets the DSCP value for RADIUS accounting
nai-routing	Optional. Disables *Network Access Identifier* (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 generated RADIUS accounting packets to its default

`no attribute framed-mtu`

no attribute framed-mtu	Resets Framed-MTU RADIUS server attribute in access and accounting requests

`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
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|nai-routing|proxy-mode|retry-timeout-factor|timeout}`

no authentication server <1-6>	Resets the accounting server preference for the server specified by the index <1-6>
dscp	Optional. Resets the DSCP value for RADIUS authentication
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 the server health check interval value 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 wireless 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 being used in a 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 brocade port 1009
 authentication server 5 timeout 10
 accounting server 2 host 172.16.10.10 secret 0 brocade 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 brocade port 1009
 authentication server 5 timeout 10
 accounting server 2 host 172.16.10.10 secret 0 brocade 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers – Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 originator of the RADIUS request as the NAS identifier. The originator could be an AP or wireless controller with radio. • proxier – Configures the proxying device as the NAS identifier. The device could be a wireless 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 wireless 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers – Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
server-pooling-mode [failover|load-balance]
```

Parameters

```
server-pooling-mode [failover|load-balance]
```

failover	Sets the pooling mode to failover 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.

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 brocade port 1009
 authentication server 5 timeout 10
 accounting server 2 host 172.16.10.10 secret 0 brocade 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, to default

use

aaa-policy

Applies a *Network Access Control* (NAC) list for use by this AAA policy. This allows only the set of configured devices to use AAA servers.

For more information on creating a NAC list, see *nac-list*.

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers – Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
use nac-list <NAC-LIST-NAME>
```

Parameters

```
use nac-list <NAC-LIST-NAME>
```

nac-list <NAC-LIST-NAME>	Configures a NAC for use with the AAA policy • <NAC-LIST-NAME> – Specify the NAC list name.

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 brocade port 1009
 authentication server 5 timeout 10
 accounting server 2 host 172.16.10.10 secret 0 brocade 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

In this chapter

This chapter summarizes the auto provisioning policy commands in the CLI command structure.

Adoption rules are sorted by precedence value and matched (filtered) against the information available from an AP. Any rule for the wrong AP type is ignored.

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.

Use the (config) instance to configure auto-provisioning-policy commands. To navigate to the auto-provisioning-policy instance, use the following commands:

```
RFSSwitch(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

  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 36 summarizes auto provisioning policy configuration commands.

TABLE 36 Auto-Provisioning-Policy-Config Commands

Command	Description	Reference
adopt	Adds rules for device adoption	*page 9-622*
default-adoption	Adopts devices even when no matching rules are found. Assigns default profile and default RF Domain	*page 9-625*
deny	Adds a rule to deny device adoption	*page 9-625*
no	Negates a command or reverts settings to their default	*page 9-627*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
do	Runs commands from the EXEC mode	*page 4-165*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes information to memory or terminal	*page 5-310*

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
adopt [br650|br6511|br71xx]

adopt [br650|br6511|br71xx] precedence <1-10000>
          [profile|rf-domain]

adopt [br650|br6511|br71xx]
          precedence <1-10000> [profile <DEVICE-PROFILE-NAME>|rf-domain
<RF-DOMAIN-NAME>]
          [any|cdp-match|dhcp-option|fqdn|ip|lldp-match|mac|model-number|
serial-number|vlan]
```

```
adopt [br650|br6511|br71xx]
          precedence <1-10000> [profile <DEVICE-PROFILE-NAME>|rf-domain
<RF-DOMAIN-NAME>] any

adopt [br650|br6511|br71xx] 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>|vlan <VLAN-ID>]
```

Parameters

```
adopt [br650|br6511|br71xx]
precedence <1-10000> [profile <DEVICE-PROFILE-NAME>|rf-domain
<RF-DOMAIN-NAME>] any
```

br650	Sets AP adoption type as Brocade Mobility 650 Access Point
br6511	Sets AP adoption type as Brocade Mobility 6511 Access Point
br71xx	Sets AP adoption type as Brocade Mobility 71XX Access Point
precedence <1-10000>	Sets the rule precedence from 1 - 10000. A rule with a lower value has a higher precedence in execution.
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.
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
any	Indicates any device. Any device that meets the criteria defined is allowed to adopt to the wireless controller.

```
adopt [br650|br6511|br71xx]
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>|
vlan <VLAN-ID>]
```

br6511	Sets the AP adoption type as Brocade Mobility 6511 Access Point
br71xx	Sets the AP adoption type as Brocade Mobility 71XX Access Point
precedence <1-10000>	Sets the rule precedence. A rule with a lower value has a higher precedence in execution.
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.
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 RF Domain
cdp-match <LOCATION-SUBSTRING>	Adopts any device based on the *CISCO Discovery Protocol* (CDP) snoop match • <LOCATION-SUBSTRING> – Specify the value to match.

dhcp-option <DHCP-OPTION>	DHCP options are used to 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. This parameter allows a device to adopt based on its DHCP option. • <DHCP-OPTION> – Specify the DHCP option value to match.
fqdn <FQDN>	*Fully Qualified Domain Name* (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 name to match.
ip [<START-IP> <END-IP>| <IP/MASK>]	Adopts a device if it matches the range of IP addresses, or is part of a 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>	*Link Layer Discovery Protocol* (LLDP) is a vendor neutral link layer protocol used to advertise a network device's identity, capabilities, and neighbors on a local area network. This parameter allows a device to adopt based on its LLDP information. • <LLDP-STRING> – Specify the LLDP information to match.
mac <START-MAC> {<END-MAC>}	Adopts a device if it matches the range of MAC addresses • <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 to match.
serial-number <SERIAL-NUMBER>	Adopts a device if its serial number matches <SERIAL-NUMBER> • <SERIAL-NUMBER> – Specify the serial number to match.
vlan <VLAN-ID>	Adopts a device if its VLAN matches <VLAN-ID> • <VLAN-ID> – Specify the VLAN ID to match.

Example

```
rfs7000-37FABE(config-auto-provisioning-policy-test)#adopt br7131 10 br7131
default vlan 1

rfs7000-37FABE(config-auto-provisioning-policy-test)#commit write memory

rfs7000-37FABE(config-auto-provisioning-policy-test)#show wireless ap
+---+---------------+---------+-------------+--------------+
|IDX|NAME |MAC |TYPE|SERIAL-NUMBER |ADOPTION-MODE|   VERSION    |
+---+---------------+---------+-------------+--------------+
| 1 | br7131-889EC4 | 00-15-70-88-9E-C4 | br7131 | 8164520900006 | L2: vlan1
| 5.2.0.0-033D |
+---+---------------+------------------+--------+---------------+--------


rfs7000-37FABE(config-auto-provisioning-policy-test)#show wireless ap
configured
+-----+-----------------+--------------------+------------------+--------
| IDX |       NAME      |        MAC         |     PROFILE      |  RF-DOMAIN  |
+-----+-----------------+--------------------+------------------+--------
| 1   | br7131-889EC4   | 00-15-70-88-9E-C4   | default-br7131   | default
|
| 2   | br650-445566    | 11-22-33-44-55-66   | default-br650    | default     |
+-----+-----------------+--------------------+------------------+--------
```

```
rfs7000-37FABE(config-auto-provisioning-policy-test)#adopt br7131 10 br7131
default dhcp-option test
rfs7000-37FABE(config-auto-provisioning-policy-test)#adopt br7131 10 br7131
default ip 172.16.10.3 172.16.10.4
rfs7000-37FABE(config-auto-provisioning-policy-test)#adopt br7131 10 br7131
default ip 172.16.10.3/24
rfs7000-37FABE(config-auto-provisioning-policy-test)#adopt br7131 10 br7131
default mac 11-22-33-44-55-66
rfs7000-37FABE(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
 adopt br7131 10 br7131 default vlan 1
rfs7000-37FABE(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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
default-adoption
```

Parameters

None

Example

```
rfs7000-37FABE(config-auto-provisioning-policy-test)#default-adoption

rfs7000-37FABE(config-auto-provisioning-policy-test1)#show context
auto-provisioning-policy test1
 default-adoption
 adopt br71xx precedence 10 profile br7131 rf-domain default vlan 1
rfs7000-37FABE(config-auto-provisioning-policy-test1)#
```

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
deny [br650|br6511|br71xx]

deny [br650|br6511|br71xx]
          [any|cdp-match|dhcp-option|fqdn|ip|lldp-match|mac|model-number|
serial-number|vlan]

deny [br650|br6511|br71xx] precedence <1-10000> any

deny [br650|br6511|br71xx]
          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 [br650|br6511|br71xx] precedence <1-10000> any
```

br650	Sets AP type as Brocade Mobility 650 Access Point
br6511	Sets AP type as Brocade Mobility 6511 Access Point
br71xx	Sets AP type as Brocade Mobility 71XX Access Point
precedence <1-10000>	Sets the rule precedence. A rule with a lower value has a higher precedence in execution.
any	Indicates any device. Any device that meets the criteria defined is not allowed to adopt to the wireless controller.

```
deny [br650|br6511|br71xx] 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>]
```

br650	Sets AP type as Brocade Mobility 650 Access Point
br6511	Sets AP type as Brocade Mobility 6511 Access Point
br71xx	Sets AP type as Brocade Mobility 71XX Access Point
precedence <1-10000>	Sets the rule precedence. A rule with a lower value has a higher precedence in execution.
cdp-match <LOCATIO-SUBSTRING>	Denies adoption based on the *CISCO Discovery Protocol* (CDP) snoop match • <LOCATION-SUBSTRING> – Specify the value to match.

dhcp-option <DHCP-OPTION>	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. This parameter denies adoption to a device based on its DHCP option. • <DHCP-OPTION> – Specify the DHCP option value.
fqdn <FQDN>	*Fully Qualified Domain Name* (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 denies adoption based on the fully qualified domain name of the device. • <FQDN> – Specify the FQDN to match.
ip [<START-IP> <END-IP>|<IP/MASK>]	Adopts a device if it matches the range of IP addresses or is part of a 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>	LLDP is a vendor neutral link layer protocol used to advertise a network device's identity, capabilities, and neighbors on a local area network. This parameter denies adoption to a device based on its LLDP information. • <LLDP-STRING> – Specify the LLDP information to match.
mac <START-MAC> {<END-MAC>}	Adopts a device if it matches a single MAC address or a range of MAC addresses • <START-MAC> – Specify the first IP address in the range. Provide this MAC address if you want to match for a single device. • <END-MAC> – Optional. Specify the last IP address in the range.
model-number <MODEL-NUMBER>	Adopts a device if its model number matches <MODEL-NUMBER> • <MODEL-NUMBER> – Specify the model number to match.
serial-number <SERIAL-NUMBER>	Adopts a device if its serial number matches <SERIAL-NUMBER> • <SERIAL-NUMBER> – Specify the serial number to match.
vlan <VLAN-ID>	Adopts a device if its VLAN matches <VLAN-ID> • <VLAN-ID> – Specify the VLAN ID to match.

Example

```
rfs7000-37FABE(config-auto-provisioning-policy-test)#deny br7131 600 vlan 1

rfs7000-37FABE(config-auto-provisioning-policy-test)#deny br7131 600 ip
172.16.10.1/24

rfs7000-37FABE(config-auto-provisioning-policy-test1)#show context
auto-provisioning-policy test1
 default-adoption
 adopt br71xx precedence 10 profile br7131 rf-domain default vlan 1
 deny br71xx 100 vlan 20
 deny br71xx precedence 600 ip 172.16.10.1/24
rfs7000-37FABE(config-auto-provisioning-policy-test1)#
```

Related Commands:

no	Removes a deny rule

no

auto-provisioning-policy

Negates an auto provisioning 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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
no [adopt|default-adoption|deny]

no adopt precedence <1-1000>
no deny precedence <1-1000>
no default-adoption
```

Parameters

```
no adopt precedence <1-1000>
```

adopt precedence <1-1000>	Removes an adoption rule from the list of rules based on its rule precedence • precedence <1-1000> – Specify the rule precedence.

```
no deny precedence<1-1000>
```

deny precedence <1-1000>	Removes an deny rule from the list of rules based on its rule precedence • precedence <1-1000> – Specify the rule precedence.

```
no default-adoption
```

default-adoption	Removes the default adoption rule. When the default adoption rule is absent, devices are not adopted

Example

```
rfs7000-37FABE(config-auto-provisioning-policy-test1)#no default-adoption
rfs7000-37FABE(config-auto-provisioning-policy-test1)#
```

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

Chapter

Advanced-WIPS-Policy

10

In this chapter

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) 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:

```
RFSSwitch(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 37 summarizes advanced WIPS policy configuration commands.

TABLE 37 Advanced-WIPS-Policy-Config Commands

Command	Description	Reference
event	Configures event monitoring settings	*page 10-631*
no	Negates a command or sets its default	*page 10-636*
server-listen-port	Sets a local WIPS server's listening port	*page 10-638*
terminate	Adds a device to a list of terminated devices	*page 10-639*
use	Defines the settings used with the advanced WIPS policy	*page 10-639*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
do	Runs commands from the EXEC mode	*page 4-165*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes information to memory or terminal	*page 5-310*

event

advanced-wips-policy

Configures anomalous frame detection in a RF network

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
event [accidental-association|all|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-ap-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-
dected|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-
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)}


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-ap <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-ap-detection mitigation-enable
event rogue-ap-detection trigger-against
[neighboring|sanctioned|unsanctioned]
          {(neighboring|sanctioned|unsanctioned)}
```

Parameters

```
event accidental-association mitigation-enable
```

accidental-association	This event occurs when a client associates accidentally
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 a client accidentally associates to a 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-
dected|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-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-disassociation-detection	This event occurs when DoS disassociation is detected
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 wireless 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.
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-ap <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-ap <0-65535>| eapol-start-frames-mu <0-65535>]	Sets the EAPOL logoff frames flood threshold • eapol-start-frames-ap – 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-ap-detection mitigation-enable`

rogue-ap-detection	This event occurs when rogue APs are detected in the network
mitigation-enable	Enables default mitigation for the rogue-ap-detection event

`event rogue-ap-detection trigger-against [neighboring|sanctioned|unsanctioned] {(neighboring|sanctioned|unsanctioned)}`

rogue-ap-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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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>
```

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
```

server-listen-port	Resets the listen port for WIPS sensors to its default

```
no terminate <MAC>
```

terminate <MAC>	Removes a device by its MAC address <MAC> from the device termination list

```
no use device-configuration
```

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 WIPS server's listening port, where WIPS sensors connect to the local WIPS server

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
terminate <MAC>
```

Parameters

```
terminate <MAC>
```

terminate <MAC>	Adds a device MAC address <MAC> to the device termination list. Devices on this list cannot access the network

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 *Chapter 4,* .

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

11

Association-ACL-Policy

In this chapter

This chapter summarizes the association ACL policy commands in the CLI command structure.

Use the (config) instance to configure association ACL policy related configuration commands. To navigate to the association-acl-policy instance, use the following commands:

```
RFSSwitch(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)#
```

association-acl-policy

Table 38 summarizes association ACL policy configuration commands.

TABLE 38 Association-ACL-Policy-Config Commands

Command	Description	Reference
deny	Specifies a range of denied MAC addresses	*page 11-642*
no	Negates a command or sets its default	*page 11-643*
permit	Specifies a range of permitted MAC addresses	*page 11-644*
clrscr	Clears the display screen	*page 5-275*

TABLE 38 Association-ACL-Policy-Config Commands

Command	Description	Reference
commit	Commits (saves) changes made in the current session	*page 5-276*
do	Runs commands from the EXEC mode	*page 4-165*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-165*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes information to memory or terminal	*page 5-310*

deny

association-acl-policy

Denies device access to the 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 list rules are applied. Up to a thousand (1000) deny rules can be defined.

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
deny <STARTING-MAC> [<ENDING-MAC>|precedence]

deny <STARTING-MAC> precedence <1-1000>
deny <STARING-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 checked 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 checked in an increasing order of precedence. • <1-1000> – Specify a value from 1 - 1000.

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 single device or a set of devices from the deny list

no

association-acl-policy

Negates a command or sets its default

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
no [deny|permit]

no deny <STARTING-MAC> precedence <1-1000>
no deny <STARING-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>	Sets the rule precedence. Rules are checked in an increasing order of 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>	Sets the rule precedence. Rules are checked in an increasing order of 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>	Sets the rule precedence. Rules are checked in an increasing order of 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>	Sets the rule precedence. Rules are checked in an increasing order of precedence. • <1-1000> – Specify a value from 1 - 1000.

Example

```
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

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

Permits device access to the 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) deny rules can be defined.

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
permit <STARTING-MAC> [<ENDING-MAC>|precedence]

permit <STARTING-MAC> precedence <1-1000>
permit <STARING-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>	Sets a rule precedence. Rules are checked 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>	Sets a rule precedence. Rules are checked in an increasing order of precedence. • <1-1000> – Specify a value from 1 - 1000.

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 device or a set of devices from the permit list

11

Chapter

12

Access-list

In this chapter

This chapter summarizes IP and MAC access list commands in the CLI command structure.

Access lists control access to the network using a set of rules also known as *Access Control Entries* (ACE). Each rule specifies an action taken when a packet matches a given set of rules. If the action is deny, the packet is dropped. If the action is permit, the packet is allowed. The rule is applied to a specific protocol, source/destination IP address(es), or source/destination port(s). The following ACLs are supported:

- IP access lists
- MAC access lists

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 access list commands. To navigate to the (config-access-list) instance, use the following commands:

ip-access-list

```
rfs7000-37FABE(config)#ip access-list test
rfs7000-37FABE(config-ip-acl-test)#?
ACL Configuration commands:
  deny     Specify packets to reject
  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)#
```

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
  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)#
```

ip-access-list

Table 39 summarizes IP access list configuration commands.

TABLE 39 IP-Access-List-Config Commands

Command	Description	Reference
deny	Specifies packets to reject	*page 12-648*
no	Negates a command or sets its default	*page 12-653*
permit	Permits specific packets	*page 12-658*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
do	Runs commands from the the EXEC mode	*page 4-165*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes information to memory or terminal	*page 5-310*

deny

ip-access-list

Specifies packets to reject

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
deny [icmp|ip|proto|tcp|udp]

deny icmp [<SOURCE-IP/MASK>|any|host <IP>] [<DESTINATION-IP/MASK>|any|host
<IP>]
          <ICMP-TYPE> <ICMP-CODE> [log rule-precedence <1-5000>|
rule-precedence <1-5000>]
          {(rule-description <RULE-DESCRIPTION>)}

deny ip [<SOURCE-IP/MASK>|any|host <IP>] [<DESTINATION-IP/MASK>|any|host <IP>]
          [log rule-precedence <1-5000>|rule-precedence <1-5000>]
          {(rule-description <RULE-DESCRIPTION>)}

deny proto [<PROTOCOL-NUMBER>|<PROTOCOL-NAME>|eigrp|gre|igmp|igp|ospf|vrrp]
          [<SOURCE-IP/MASK>|any|host <IP>] [<DESTINATION-IP/MASK>|any|host
<IP>]
          [log rule-precedence <1-5000>|rule-precedence <1-5000>]
          {(rule-description <RULE-DESCRIPTION>)}

deny [tcp|udp] [<SOURCE-IP/MASK>|any|host <IP>] [<DESTINATION-IP/MASK>|any|
          eq <SOURCE-PORT>|host <IP>|range <START-PORT> <END-PORT>]
          [eq [<DESTINATION-PORT>|<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-precedence <1-5000>]
          {(rule-description <RULE-DESCRIPTION>)}
```

Parameters

```
deny icmp [<SOURCE-IP/MASK>|any|host <IP>] [<DESTINATION-IP/MASK>|any|host
<IP>] <ICMP-TYPE> <ICMP-CODE> [log rule-precedence <1-5000>|rule-precedence
<1-5000>]
{(rule-description <RULE-DESCRIPTION>)}
```

icmp	Configures the ACL for *Internet Control Message Protocol* (ICMP) packets
<SOURCE-IP/MASK>	Sets the IP address and mask as the source to deny access
any	Identifies all devices as the source to deny access
host <IP>	Identifies a specific host as the source to deny access • <IP> – Specify an exact host IP address to match.
<DESTINATION-IP/MASK>	Sets the IP address and mask as the destination to deny access
any	Identifies all devices as the destination to deny access

host <IP>	Identifies a specific host as the destination to deny access • <IP> – Specify an exact host IP address to match.
<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.”
log	Logs all ICMP packets related deny events
rule-precedence <1-5000>	Sets the rule precedence. Rules are checked in an increasing order of precedence • <1-5000> – Specify the rule precedence from 1 - 5000.
rule-description <RULE-DESCRIPTION>	Optional. Defines the rule description • <RULE-DESCRIPTION> – Provide a description of the rule. The description should not exceed 128 characters.

```
deny ip [<SOURCE-IP/MASK>|any|host <IP>] [<DESTINATION-IP/MASK>|any|host <IP>]
[log rule-precedence <1-5000>|rule-precedence <1-5000>]
{(rule-description <RULE-DESCRIPTION>)}
```

ip	Configures the ACL for IP packets
<SOURCE-IP/MASK>	Sets the IP address and mask as the source to deny access
any	Identifies all devices as the source to deny access
host <IP>	Identifies a specific host as the source to deny access • <IP> – Specify an exact host IP address to match.
<DESTINATION-IP/MASK>	Sets the IP address and mask as the destination to deny access
any	Identifies all devices as the destination to deny access
host <IP>	Identifies a specific host as the destination to deny access • <IP> – Specify an exact host IP address to match.
log	Logs all IP packets related deny events
rule-precedence <1-5000>	Sets the rule precedence. Rules are checked in an increasing order of precedence • <1-5000> – Specify the rule precedence from 1 - 5000.
rule-description <RULE-DESCRIPTION>	Optional. Defines the rule description • <RULE-DESCRIPTION> – Provide a description of the rule. The description should not exceed 128 characters.

```
deny proto [<PROTOCOL-NUMBER>|<PROTOCOL-NAME>|eigrp|gre|igmp|igp|ospf|vrrp]
[<SOURCE-IP/MASK>|any|host <IP>] [<DESTINATION-IP/MASK>|any|host <IP>]
[log rule-precedence <1-5000>|rule-precedence <1-5000>]
{rule-description <RULE-DESCRIPTION>}
```

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-NAME>	Filters protocols using their IANA 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 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 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>	Sets the IP address and mask as the source to deny access
any	Identifies all devices as the source to deny access
host <IP>	Identifies a specific host as the source to deny access • <IP> – Specify the exact host IP address to match.
<DESTINATION-IP/MASK>	Sets the IP address and mask as the destination to deny access
any	Identifies all devices as the destination to deny access
host <IP>	Identifies a specific host as the destination to deny access • <IP> – Specify an exact host IP address to match.
log	Logs all protocol (other than IP, ICMP, TCP, and UDP) related deny events
rule-precedence <1-5000>	Sets the rule precedence. Rules are checked in an increasing order of precedence • <1-5000> – Specify the rule precedence from 1 - 5000.
rule-description <RULE-DESCRIPTION>	Optional. Sets the rule description • <RULE-DESCRIPTION> – Provide a description of the rule. The description should not exceed 128 characters.
	`deny [tcp|udp] [<SOURCE-IP/MASK>|any|host <IP>] [<DESTINATION-IP/MASK>|any| eq <SOURCE-PORT>|host <IP>|range <START-PORT> <END-PORT>] [eq [<DESTINATION-PORT>|<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-precedence <1-5000>] *{(rule-description <RULE-DESCRIPTION>)}*`
tcp	Configures the ACL for TCP packets
udp	Configures the ACL for UDP packets
<SOURCE-IP/MASK>	Sets the IP address and mask as the source to deny access
any	Identifies all devices as the source to deny access

host <IP>	Identifies a specific host as the source to deny access • <IP> – Specify an exact host IP address to match.
<DESTINATION-IP/MASK>	Sets the IP address and mask as the destination to deny access
any	Identifies all devices as the destination to deny access
eq <SOURCE-PORT>	Identifies a specific source port • <SOURCE-PORT> – Specify the exact source port.
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 [<DESTINATION-PORT>| <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 • <DESTINATION-PORT> – The destination port 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) Contd..
	• 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 deny events
rule-precedence <1-5000>	Sets the rule precedence. Rules are checked in an increasing order of precedence • <1-5000> – Specify the rule precedence from 1 - 5000.
rule-description <RULE-DESCRIPTION>	Optional. Sets the rule description • <RULE-DESCRIPTION> – Provide a description of the rule. The description should not exceed 128 characters.

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

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/denied based on the ACL configuration.

- Filtering TCP/UDP allows the user to specify port numbers as filtering criteria
- Select ICMP as the protocol to allow/deny ICMP packets. Selecting ICMP provides the option of filtering 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)#
```

Related Commands:

no	Removes a specified IP deny access rule

no

ip-access-list

Negates a command or sets its default

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
no [deny|permit]

no [deny|permit] [icmp|ip|proto|tcp|udp]

no [deny|permit] icmp [<SOURCE-IP/MASK>|any|host <IP>]
[<DESTINATION-IP/MASK>|any|
          host <IP>] <ICMP-TYPE> <ICMP-CODE> [log rule-precedence <1-1500>|
          rule-precedence <1-5000>] {(rule-description <RULE-DESCRIPTION>)}

no [deny|permit] ip [<SOURCE-IP/MASK>|any|host <IP>]
[<DESTINATION-IP/MASK>|any|
          host <IP>] [log rule-precedence <1-5000>|rule-precedence <1-5000>]
          {(rule-description <RULE-DESCRIPTION>)}
```

```
no [deny|permit] proto [<PROTOCOL-NUMBER>|<PROTOCOL-NAME>|eigrp|gre|igmp|igp|
          ospf|vrrp] [<SOURCE-IP/MASK>|any|host <IP>]
[<DESTINATION-IP/MASK>|any|host <IP>]
          [log rule-precedence <1-5000>|rule-precedence <1-5000>]
          {(rule-description <RULE-DESCRIPTION>)}

no [deny|permit] [tcp|udp] [<SOURCE-IP/MASK>|any|host <IP>]
[<DESTINATION-IP/MASK>|
          any|eq <SOURCE-PORT>|host <IP>|range <START-PORT> <END-PORT>]
          [eq
[<DESTINATION-PORT>|<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-precedence <1-5000>]
          {(rule-description <RULE-DESCRIPTION>)}
```

Parameters

```
no [deny|permit] icmp [<SOURCE-IP/MASK>|any|host <IP>]
[<DESTINATION-IP/MASK>|any|
host <IP>] <ICMP-TYPE> <ICMP-CODE> [log rule-precedence <1-1500>|
rule-precedence <1-5000>] {(rule-description <RULE-DESCRIPTION>)}
```

no deny	Removes a deny rule
no permit	Removes a permit rule
icmp	Removes the ACL for ICMP packets
<SOURCE-IP/MASK>	Sets the IP address and mask as the source to permit/deny access
any	Identifies all devices as the source to permit/deny access
host <IP>	Identifies a specific host as the source to permit/deny access • <IP> – Specify an exact host IP address to match.
<DESTINATION-IP/MASK>	Sets the IP address and mask as the destination to permit/deny access
any	Identifies all devices as the destination to permit/deny access
host <IP>	Identifies a specific host as the destination to permit/deny access • <IP> – Specify an exact host IP address to match.
<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.”
log	Logs all permit/deny events
rule-precedence <1-5000>	Sets the rule precedence. Rules are checked in the order of their rule precedence • <1-5000> – Specify the rule precedence from 1 - 5000.
rule-description <RULE-DESCRIPTION>	Optional. Sets the rule description • <RULE-DESCRIPTION> – Provide a description of the rule. The description should not exceed 128 characters.

```
no [deny|permit] ip [<SOURCE-IP/MASK>|any|host <IP>]
[<DESTINATION-IP/MASK>|any|
host <IP>] [log rule-precedence <1-5000>|rule-precedence <1-5000>]
{(rule-description <RULE-DESCRIPTION>)}
```

no deny	Removes a deny rule
no permit	Removes a permit rule
ip	Removes the ACL for IP packets
<SOURCE-IP/MASK>	Sets the IP address and mask as the source to permit/deny access
any	Identifies all devices as the source to permit/deny access
host <IP>	Identifies a specific host as the source to permit/deny access • <IP> – Specify an exact host IP address to match.
<DESTINATION-IP/MASK>	Sets the IP address and mask as the destination to permit/deny access
any	Identifies all devices as the destination to permit/deny access
host <IP>	Identifies a specific host as the destination to permit/deny access • <IP> – Specify an exact host IP address to match.
log	Logs all permit/deny events
rule-precedence <1-5000>	Sets the rule precedence. Rules are checked in the order of their rule precedence • <1-5000> – Specify the rule precedence from 1 - 5000.
rule-description <RULE-DESCRIPTION>	Optional. Sets the rule description • <RULE-DESCRIPTION> – Provide a description of the rule. The description should not exceed 128 characters.

```
no [deny|permit] proto [<PROTOCOL-NUMBER>|<PROTOCOL-NAME>|eigrp|gre|igmp|igp|
ospf|vrrp] [<SOURCE-IP/MASK>|any|host <IP>] [<DESTINATION-IP/MASK>|any|host
<IP>]
[log rule-precedence <1-5000>|rule-precedence <1-5000>]
{(rule-description <RULE-DESCRIPTION>)}
```

no deny	Removes a deny rule
no permit	Removes a permit rule
proto	Removes ACLs for additional protocols Additional protocols (other than IP, ICMP, TCP, and UDP) must be removed using this parameter
<PROTOCOL-NUMBER>	Identifies protocol by the IANA protocol number
<PROTOCOL-NAME>	Identifies protocol by the IANA protocol name
eigrp	Identifies the *Enhanced Interior Gateway Protocol* (EIGRP) protocol 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 *Generic Routing Encapsulation* (GRE) protocol GRE is 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 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 *Interior Gateway Protocol* (IGP) (primarily used by CISCO for their IGRP) IGP enables exchange of information between hosts and routers within a managed network. The most commonly used IGP protocols are: *Routing Information Protocol* (RIP) and *Open Shortest Path First* (OSPF)
ospf	Identifies the OSPF protocol 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 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>	Sets the IP address and mask as the source to permit/deny access
any	Identifies all devices as the source to permit/deny access
host <IP>	Identifies a specific host as the source to permit/deny access • <IP> – Specify an exact host IP address to match.
<DESTINATION-IP/MASK>	Sets the IP address and mask as the destination to permit/deny access
any	Identifies all devices as the destination to permit/deny access
host <IP>	Identifies a specific host as the destination to permit/deny access • <IP> – Specify the exact host IP address to match.
log	Logs all permit/deny events
mark [8021p <0-7>| dscp <0-63>]	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>	Sets the rule precedence. Rules are checked in the order of their rule precedence • <1-5000> – Specify the rule precedence from 1 - 5000.
rule-description <RULE-DESCRIPTION>	Optional. Sets the rule description • <RULE-DESCRIPTION> – Provide a description of the rule. The description should not exceed 128 characters.

```
no [deny|permit] [tcp|udp] [<SOURCE-IP/MASK>|any|host <IP>]
[<DESTINATION-IP/MASK>|
any|eq <SOURCE-PORT>|host <IP>|range <START-PORT> <END-PORT>]
[eq
[<DESTINATION-PORT>|<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-precedence <1-5000>]
{(rule-description <RULE-DESCRIPTION>)}
```

no deny	Removes a deny rule
no permit	Removes a permit rule
tcp	Removes the ACL for TCP packets
udp	Removes the ACL for UDP packets
<SOURCE-IP/MASK>	Sets the IP address and mask as the source to permit/deny access
any	Identifies all devices as the source to permit/deny access
host <IP>	Identifies a specific host as the source to permit/deny access • <IP> – Specify an exact host IP address to match.

<DESTINATION-IP/MASK>	Sets the IP address and mask as the destination to permit/deny access
any	Identifies all devices as the destination to permit/deny access
host <IP>	Identifies a specific host as the destination to permit/deny access • <IP> – Specify an exact host IP address to match.
eq <SOURCE-PORT>	Specifies a specific source port to match • <SOURCE-PORT> – Specify the source port
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 [<DESTINATION-PORT>| <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 • <DESTINATION-PORT> – The destination port designated by its number • <SERVICE-NAME> – The service name • bgp – The designated BGP protocol port • dns – The designated DNS protocol port • ftp – The designated FTP protocol port • ftp-data – The designated FTP data port • gropher – The designated GROPHER protocol port • https – The designated HTTPS protocol port • ldap – The designated LDAP protocol port • nntp – The designated NNTP protocol port • ntp – The designated NTP protocol port • pop3 – The designated POP3 protocol port • sip – The designated SIP protocol port • smtp – The designated SMTP protocol port • ssh – The designated SSH protocol port • telnet – The designated Telnet protocol port • tftp – The designated TFTP protocol port • www – The designated www protocol port
range <START-PORT> <END-PORT>	Identifies 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/deny events
rule-precedence <1-5000>	Sets the rule precedence. Rules are checked in the order of their rule precedence • <1-5000> – Specify the rule precedence from 1 - 5000.
rule-description <RULE-DESCRIPTION>	Optional. Sets the rule description • <RULE-DESCRIPTION> – Provide a description of the rule. The description should not exceed 128 characters.

Usage Guidelines:

Removes an access list control entry. Provide the rule-precedence value when using the no command.

Example

```
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

rfs7000-37FABE(config-ip-acl-test)#show context
ip access-list test
rfs7000-37FABE(config-ip-acl-test)#
```

Related Commands:

deny	Creates a deny ACL
permit	Creates a permit ACL

permit

ip-access-list

Permits specific packets

NOTE
Use a decimal value representation to implement a `permit/deny` designation for a packet. The command set for IP 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
permit [icmp|ip|proto|tcp|udp]

permit icmp [<SOURCE-IP/MASK>|any|host <IP>] [<DESTINATION-IP/MASK>|any|host
<IP>]
          <ICMP-TYPE> <ICMP-CODE> (log,mark [8021p <0-7>|dscp <0-63>],
          rule-precedence <1-5000>) {(rule-description <RULE-DESCRIPTION>)}

permit ip [<SOURCE-IP/MASK>|any|host <IP>] [<DESTINATION-IP/MASK>|any|host
<IP>]
          (log,mark [8021p <0-7>|dscp <0-63>],rule-precedence <1-5000>)
          {(rule-description <RULE-DESCRIPTION>)}

permit proto [<PROTOCOL-NUMBER>|<PROTOCOL-NAME>|eigrp|gre|igmp|igp|ospf|vrrp]
          [<SOURCE-IP/MASK>|any|host <IP>] [<DESTINATION-IP/MASK>|any|host
<IP>]
          (log,mark [8021p <0-7>|dscp <0-63>],rule-precedence <1-5000>)
          {(rule-description <RULE-DESCRIPTION>)}

permit [tcp|udp] [<SOURCE-IP/MASK>|any|host <IP>] [<DESTINATION-IP/MASK>|any|
          eq <SOURCE-PORT>|host <IP>|range <START-PORT> <END-PORT>]
          [eq
[<DESTINATION-PORT>|<SERVICE-NAME>|bgp|dns|ftp|ftp-data|gopher|https|ldap|
```

```
            nntp|ntp|pop3|sip|smtp|ssh|telnet|tftp|www]|log|mark [8021p
<0-7>|dscp <0-63>]|
            range <START-PORT> <END-PORT>|rule-precedence <1-5000>]
            {(rule-description <RULE-DESCRIPTION>)}
```

Parameters

```
permit icmp [<SOURCE-IP/MASK>|any|host <IP>] [<DESTINATION-IP/MASK>|any|host
<IP>]
<ICMP-TYPE> <ICMP-CODE> (log|mark [8021p <0-7>|dscp <0-63>]|
rule-precedence <1-5000>) {(rule-description <RULE-DESCRIPTION>)}
```

icmp	Configures an ACL for ICMP packets
<SOURCE-IP/MASK>	Sets the IP address and mask as the source to permit access
any	Permits traffic from all potential sources
host <IP>	Permits traffic from a specific host • <IP> – Specify an exact host IP address to match.
<DESTINATION-IP/MASK>	Sets the IP address and mask as the destination to permit access
any	Permits traffic to all destinations
host <IP>	Permits traffic to a specific host • <IP> – Specify an exact host IP address to match.
<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.”
log	Logs all permit events
mark [8021p <0-7>| dscp <0-63>]	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>	Sets the rule precedence. Rules are checked in the order of their rule precedence • <1-5000> – Specify the rule precedence from 1 - 5000.
rule-description <RULE-DESCRIPTION>	Optional. Sets the rule description • <RULE-DESCRIPTION> – Provide a description of the rule. The description should not exceed 128 characters.

```
permit ip [<SOURCE-IP/MASK>|any|host <IP>] [<DESTINATION-IP/MASK>|any|host
<IP>]
(log,mark [8021p <0-7>|dscp <0-63>],rule-precedence <1-5000>)
{(rule-description <RULE-DESCRIPTION>)}
```

ip	Configures an ACL for IP packets
<SOURCE-IP/MASK>	Sets the IP address and mask as the source to permit access
any	Permits traffic from all potential sources
host <IP>	Permits traffic from a specific host • <IP> – Specify an exact host IP address to match.
<DESTINATION-IP/MASK>	Sets the IP address and mask as the destination to permit access
any	Permits traffic to all destinations

host <IP>	Permits traffic to a specific host • <IP> – Specify an exact host IP address to match.
log	Logs all permit events
mark [8021p <0-7>| dscp <0-63>]	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>	Sets the rule precedence. Rules are checked in the order of their rule precedence • <1-5000> – Specify the rule precedence from 1 - 5000.
rule-description <RULE-DESCRIPTION>	Optional. Sets the rule description • <RULE-DESCRIPTION> – Provide a description of the rule. The description should not exceed 128 characters.

```
permit proto [<PROTOCOL-NUMBER>|<PROTOCOL-NAME>|eigrp|gre|igmp|igp|ospf|vrrp]
[<SOURCE-IP/MASK>|any|host <IP>] [<DESTINATION-IP/MASK>|any|host <IP>]
(log,mark [8021p <0-7>|dscp <0-63>],rule-precedence <1-5000>)
{(rule-description <RULE-DESCRIPTION>)}
```

proto	Configures an ACL for additional protocols Other protocols (other than IP, ICMP, TCP, and UDP) must be configured using this parameter.
<PROTOCOL-NUMBER>	Filters protocols using their IANA protocol number
<PROTOCOL-NAME>	Filters protocols using their IANA protocol name
eigrp	Identifies the EIGRP protocol 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 GRE is 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 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) IGP enables exchange of information between hosts and routers within a managed network. The most commonly used IGP protocols are: *Routing Information Protocol* (RIP) and *Open Shortest Path First* (OSPF)
ospf	Identifies the OSPF protocol 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 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>	Sets the IP address and mask as the source to permit access

any	Permits traffic from all potential sources
host <IP>	Permits traffic from a specific host • <IP> – Specify an exact host IP address to match.
<DESTINATION-IP/MASK>	Sets the IP address and mask as the destination to permit access
any	Permits traffic to all destinations
host <IP>	Permits traffic to a specific host • <IP> – Specify an exact host IP address to match .
log	Logs all permit events
mark [8021p <0-7>| dscp <0-63>]	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>	Sets the rule precedence. Rules are checked in the order of their rule precedence • <1-5000> – Specify the rule precedence from 1 - 5000.
rule-description <RULE-DESCRIPTION>	Optional. Sets the rule description • <RULE-DESCRIPTION> – Provide a description of the rule. The description should not exceed 128 characters.

```
permit [tcp|udp] [<SOURCE-IP/MASK>|any|host <IP>] [<DESTINATION-IP/MASK>|any|
eq <SOURCE-PORT>|host <IP>|range <START-PORT> <END-PORT>]
[eq
[<DESTINATION-PORT>|<SERVICE-NAME>|bgp|dns|ftp|ftp-data|gopher|https|ldap|
nntp|ntp|pop3|sip|smtp|ssh|telnet|tftp|www]|log|mark [8021p <0-7>|dscp
<0-63>]|
range <START-PORT> <END-PORT>|rule-precedence <1-5000>]
{(rule-description <RULE-DESCRIPTION>)}
```

tcp	Configures an IP ACL for TCP packets
udp	Configures an IP ACL for UDP packets
<SOURCE-IP/MASK>	Sets an IP address and mask as the source to permit access
any	Permits traffic from all potential sources
host <IP>	Permits traffic from a specific host • <IP> – Specify an exact host IP address to match.
<DESTINATION-IP/MASK>	Sets an IP address and mask as the destination to permit access
any	Permits traffic to all destinations
host <IP>	Permits traffic to a specific host • <IP> – Specify an exact host IP address to match.
eq <SOURCE-PORT>	Identifies a specific source port • <SOURCE-PORT> – Specify the source port.
range <START-PORT> <END-PORT>	Identifies a range of source ports • <START-PORT> – Specify the first port in the range. • <END-PORT> – Specify the last port in the range.

eq [<DESTINATION-PORT>| <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 • <DESTINATION-PORT> – Specify the destination port designated by its number • <SERVICE-NAME> – Specify the service name • bgp – Specifies the designated BGP protocol port • dns – Specifies the designated DNS protocol port • ftp – Specifies the designated FTP protocol port • ftp-data – Specifies the designated FTP data port • gropher – Specifies the designated GROPHER protocol port • https – Specifies the designated HTTPS protocol port • ldap – Specifies the designated LDAP protocol port • nntp – Specifies the designated NNTP protocol port • ntp – Specify the designated NTP protocol port • pop3 – Specifies the designated POP3 protocol port • sip – Specifies the designated SIP protocol port • smtp – Specifies the designated SMTP protocol port • ssh – Specifies the designated SSH protocol port • telnet – Specifies the designated Telnet protocol port • tftp – Specifies the designated TFTP protocol port • www – Specifies the designated www protocol port
range <START-PORT> <END-PORT>	Identifies 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
mark [8021p <0-7>| dscp <0-63>]	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>	Sets the rule precedence. Rules are checked in the order of their rule precedence • <1-5000> – Specify the rule precedence from 1 - 5000.
rule-description <RULE-DESCRIPTION>	Optional. Sets the rule description • <RULE-DESCRIPTION> – Provide a description of the rule. The description should not exceed 128 characters.

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

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 based on the ACL configuration.

- Filtering on TCP/UDP allows the user to specify port numbers as filtering criteria
- Select ICMP to allow/deny packets
- Selecting ICMP allows the filter of ICMP packets based on type and node.

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

mac-access-list

Table 40 summarizes MAC Access list configuration commands.

TABLE 40 MAC-Access-List-Config Commands

Command	Description	Reference
deny	Use this command to specify packets to reject	*page 12-664*
no	Negates a command or reverts settings to their default	*page 12-666*
permit	Use this command to specify packets to accept	*page 12-668*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
do	Runs commands from the EXEC mode	*page 4-165*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes information to memory or terminal	*page 5-310*

deny

mac-access-list

Specifies packets to reject

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
deny [<SOURCE-MAC>|any|host]

deny [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host <MAC>]
          [<DESTINATION-MAC> <DESTINATION-MAC-MASK>|any|host <MAC>]
          (dot1p <0-7>,log rule-precedence <1-5000>,type
[8021q|<1-65535>|aarp|appletalk|
          arp|ip|ipv6|ipx|mint|rarp|wisp],vlan <1-4095>)
          [log rule-precedence <1-5000>|rule-precedence <1-5000>]
          {(rule-description <RULE-DESCRIPTION>)}
```

Parameters

```
deny [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host <MAC>]
       [<DESTINATION-MAC> <DESTINATION-MAC-MASK>|any|host <MAC>]
(dot1p <0-7>,log rule-precedence <1-5000>,type
[8021q|<1-65535>|aarp|appletalk|
arp|ip|ipv6|ipx|mint|rarp|wisp],vlan <1-4095>)
[log rule-precedence <1-5000>|rule-precedence <1-5000>]
{(rule-description <RULE-DESCRIPTION>)}
```

<SOURCE-MAC>	Configures the source MAC address for this ACL
<SOURCE-MAC-MASK>	Configures the source MAC address mask
any	Identifies all devices as the source to deny access
host <MAC>	Identifies a specific host as the source to deny access • <MAC> – Specify an exact MAC address of the host to match.
<DESTINATION-IP/MASK>	Sets the IP address and mask as the destination to deny access
any	Identifies all devices as the destination to deny access
host <MAC>	Identifies a specific host as the destination deny access • <MAC> – Specify an exact MAC address of the host to match.
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
rule-precedence <1-5000>	Sets the rule precedence. Rules are checked in the order of their rule precedence • <1-5000> – Specify the rule precedence from 1 - 5000.
rule-description <RULE-DESCRIPTION>	Optional. Sets the rule description • <RULE-DESCRIPTION> – Provide a description of the rule. The description should not exceed 128 characters.

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/denied based on the ACL's configuration.

Example

```
rfs7000-37FABE(config-mac-acl-test)#deny 41-85-45-89-66-77 44-22-55-88-77-99
any vlan 1 log rule-precedence 2 rule-description test
rfs7000-37FABE(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 example below 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

no

mac-access-list

Negates a command or sets its default

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
no [deny|permit]

no [deny|permit] [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host <MAC>]
          [<DESTINATION-MAC> <DESTINATION-MAC-MASK>|any|host <MAC>]
          (dot1p <0-7>,log rule-precedence <1-5000>,rule-precedence <1-5000>|
          type
[8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp],vlan
<1-4095>)
          [log rule-precedence <1-5000>|rule-precedence <1-5000>]
          {(rule-description <RULE-DESCRIPTION>)}
```

Parameters

```
no [deny|permit] [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host <MAC>]
       [<DESTINATION-MAC> <DESTINATION-MAC-MASK>|any|host <MAC>]
(dot1p <0-7>,log rule-precedence <1-5000>,rule-precedence <1-5000>|
type [8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp],vlan
<1-4095>)
[log rule-precedence <1-5000>|rule-precedence <1-5000>]
{(rule-description <RULE-DESCRIPTION>)}
```

<SOURCE-MAC>	Configures the source MAC address for this ACL
<SOURCE-MAC-MASK>	Configures the source MAC address mask
any	Identifies all devices as the source to deny/permit access
host <MAC>	Identifies a specific host as the source to deny/permit access • <MAC> – Specify an exact host MAC address to match.
<DESTINATION-IP/MASK>	Sets the IP address and mask as the destination to deny/permit access
any	Identifies all devices as the destination to deny/permit access

host <MAC>	Identifies a specific host as the destination to deny/permit access • <MAC> – Specify an exact host MAC address to match.
dotp1p <0-7>	Configures the 802.1p priority value. Sets the service classes for traffic handling • <0-7> – Specify the 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 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 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.
log	Logs all deny/permit events
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>	Sets the rule precedence. Rules are checked in the order of their rule precedence • <1-5000> – Specify the rule precedence from 1 - 5000.
rule-description <RULE-DESCRIPTION>	Optional. Sets the rule description • <RULE-DESCRIPTION> – Provide a description of the rule. The description should not exceed 128 characters.

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

ip-access-list

Configures a permit MAC ACL

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
permit [<SOURCE-MAC>|any|host]

permit [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host <MAC>]
          [<DESTINATION-MAC> <DESTINATION-MAC-MASK>|any|host <MAC>]
          (dot1p <0-7>,log mark [8021p <0-7>|dscp <0-63>]|mark [8021p
<0-7>|dscp <0-63>]|
          rule-precedence <1-5000>|type
[8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|
          ipx|mint|rarp|wisp],vlan <1-4095>) {(rule-description
<RULE-DESCRIPTION>)}
```

Parameters

```
permit [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host <MAC>]
[<DESTINATION-MAC> <DESTINATION-MAC-MASK>|any|host <MAC>]
(dot1p <0-7>,log mark [8021p <0-7>|dscp <0-63>]|mark [8021p <0-7>|dscp
<0-63>]|
rule-precedence <1-5000>|type [8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|
ipx|mint|rarp|wisp],vlan <1-4095>) {(rule-description <RULE-DESCRIPTION>)}
```

<SOURCE-MAC>	Configures the source MAC address for this ACL
<SOURCE-MAC-MASK>	Configures the source MAC address' mask
any	Identifies all devices as the source to permit access
host <MAC>	Identifies a specific host as the source of traffic to permit access • <MAC> – Specify an exact host MAC address to match.
<DESTINATION-IP/MASK>	Sets the IP address and mask as the destination to permit access
any	Identifies all devices as the destination to permit access
host <MAC>	Identifies a specific host as the destination to permit access • <MAC> – Specify an exact host MAC address to match.
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 • <1-65535> – Indicates the EtherType protocol number • aarp – Indicates the AARP payload • appletalk – Indicates the Appletalk Protocol payload • arp – Indicates the ARP payload • ip – Indicates the Internet Protocol, Version 4 (IPv4) payload • ipv6 – Indicates the Internet Protocol, Version 6 (IPv6) payload • ipx – Indicates the Novell's IPX payload • mint – Indicates the MiNT protocol payload • rarp – Indicates the Reverse Address Resolution Protocol payload • wisp – Indicates the WISP payload
vlan <1-4095>	Configures the VLAN where the traffic is received • <1-4095> – Specify the VLAN ID from 1- 4095.
log	Logs all permit events
mark [8021p <0-7>| dscp <0-63>]	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>	Sets the rule precedence. Rules are checked in the order of their rule precedence • <1-5000> – Specify the rule precedence from 1 - 5000.
rule-description <RULE-DESCRIPTION>	Optional. Sets the rule description • <RULE-DESCRIPTION> – Provide a description of the rule. The description should not exceed 128 characters.

Usage Guidelines:

The permit command in the MAC ACL disallows 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
```

Related Commands:

no	Removes or resets a specified MAC ACL permit rule

Chapter

DHCP-Server-Policy

13

In this chapter

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 to receive network resources. DHCP keeps track of IP address assignments, their lease times and their availability for use by clients.

Use the (config) instance to configure DHCP server policy configuration commands. To navigate to the
DHCP server policy instance, use the following commands:

```
RFSSwitch(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 41 summarizes DHCP server policy configuration commands.

TABLE 41 DHCP-Server-Policy-Config Commands

Command	Description	Reference
bootp	Configures a BOOTP specific configuration	*page 13-672*
dhcp-class	Configures a DHCP server class	*page 13-673*
dhcp-pool	Configures a DHCP server address pool	*page 13-677*
no	Negates a command or sets its default	*page 13-709*
option	Defines the DHCP option used in DHCP pools	*page 13-710*
ping	Specifies ping parameters used by a DHCP server	*page 13-711*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
do	Runs commands from the EXEC mode	*page 4-165*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes information to memory or terminal	*page 5-310*

bootp

dhcp-server-policy

Configures a BOOTP specific configuration. *Bootstrap Protocol* (BOOTP) is used by UNIX diskless workstations to obtain the network location of their boot image and IP address. A BOOTP configuration server also assigns an IP address from a configured pool of IP addresses.

Supported in the following platforms:

- Access Points — Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
bootp ignore
```

Parameters

```
bootp ignore
```

bootp ignore	Configures a BOOTP specific configuration • ignore – Configures a DHCP server 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	Removes BOOTP specific configuration

dhcp-class

dhcp-server-policy

A DHCP user class applies different DHCP settings to a set of wireless clients. These wireless clients are grouped under the same DHCP class. This class is configured on the DHCP server to provide differentiated service.

Table 42 summarizes DHCP class configuration commands.

TABLE 42 DHCP-Class Config Commands

Command	Description	Reference
dhcp-class	Configures a DHCP class and enters its configuration mode	*page 13-673*
dhcp-class-mode commands	Invokes DHCP class parameters configuration commands	*page 13-674*

dhcp-class

dhcp-class

Configures a DHCP server class and opens a new mode. For more information, see *dhcp-class-mode commands*.

Supported in the following platforms:

- Access Points — Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
dhcp-class <DHCP-CLASS-NAME>
```

Parameters

```
dhcp-class <DHCP-CLASS-NAME>
```

<DHCP-CLASS-NAME>	Configures a DHCP class. If the class does not exist, it is created.

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 class

dhcp-class-mode commands

dhcp-class

Use DHCP class mode commands to configure the parameters of the DHCP user class.

Table 43 summarizes DHCP user class configuration commands.

TABLE 43 DHCP-Class-Config-Mode Commands

Command	Description	Reference
multiple-user-class	Enables the multiple user class option	*page 13-674*
no	Negates a command or sets its default	*page 13-675*
option	Configures DHCP server options	*page 13-676*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
do	Runs commands from the EXEC mode	*page 4-165*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes information to memory or terminal	*page 5-310*

multiple-user-class

dhcp-class-mode commands

Enables a multiple user class option for the DHCP policy

Supported in the following platforms:

- Access Points — Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 DHCP policy

no

dhcp-class-mode commands

Negates a command or sets its default

Supported in the following platforms:

- Access Points — Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
no [multiple-user-class|option]
no option user-class <VALUE>
```

Parameters

```
no multiple-user-class
```

no multiple-user-class	Disables the multiple user class option with this DHCP class

```
no option user-class <VALUE>
```

no option	Removes DHCP server options
user-class <VALUE>	Removes the user class option associated with this DHCP class • VALUE> – Specify the ASCII value for the user class option.

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 the multiple user class option for the DHCP policy
option	Configures the DHCP server options for use with this DHCP user class

option

dhcp-class-mode commands

Configures the DHCP server options for use with this DHCP user class

Supported in the following platforms:

- Access Points — Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
option user-class <VALUE>
```

Parameters

```
option user-class <VALUE>
```

user-class <VALUE>	Configures the DHCP user class options • <VALUE> – Specify the ASCII value of DHCP user class option.

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 commands create and manage 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 enables the reuse of finite addresses by keeping track of their issue, release, and reissue.

The DHCP pool commands configure a finite set of IP addresses that can be assigned whenever a device joins a network.

Table 44 summarizes DHCP pool configuration mode commands.

TABLE 44 DHCP-Pool-Config Commands

Command	Description	Reference
dhcp-pool	Creates a DHCP pool and enters its configuration mode	*page 13-677*
dhcp-pool-mode commands	Summarizes DHCP pool configuration mode commands	*page 13-678*

dhcp-pool

dhcp-pool

Configures a DHCP address pool. An address pool is a set of IP addresses allocated to devices authorized to access network resources. This enables the reuse of limited IP address resources for deployment in any network. A separate instance opens where you can configure DHCP pool parameters.

Supported in the following platforms:

- Access Points — Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
dhcp-pool <POOL-NAME>
```

Parameters

```
dhcp-pool <POOL-NAME>
```

<POOL-NAME>	Configures a policy <POOL-NAME> to specify DHCP pool parameters

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 pool

dhcp-pool-mode commands

dhcp-pool

Configures the DHCP pool parameters

Table 45 summarizes DHCP pool configuration commands.

TABLE 45 DHCP-Pool-Config-Mode Commands

Command	Description	Reference
address	Specifies a range of addresses for a DHCP pool	*page 13-679*
bootfile	Assigns a bootfile name. The bootfile name can contain letters, numbers, dots and hyphens. Consecutive dots and hyphens are not permitted.	*page 13-680*
ddns	Configures dynamic DNS parameters	*page 13-680*
default-router	Configures a default router or gateway IP address for the network pool	*page 13-681*
dns-server	Sets a DNS server's IP address available to all DHCP clients connected to the DHCP pool	*page 13-682*
domain-name	Sets the domain name for the network pool	*page 13-683*
excluded-address	Prevents a DHCP server from assigning certain addresses to the DHCP pool	*page 13-684*

TABLE 45 DHCP-Pool-Config-Mode Commands

Command	Description	Reference
lease	Sets a valid lease for the IP address used by DHCP clients in the DHCP pool	*page 13-685*
netbios-name-server	Configures a NetBIOS (WINS) name server's IP address	*page 13-686*
netbios-node-type	Defines the NetBIOS node type	*page 13-686*
network	Configures the network on which the DHCP server is deployed	*page 13-687*
next-server	Configures the next server in the boot process	*page 13-688*
no	Negates a command or sets its default	*page 13-689*
option	Configures RAW DHCP options	*page 13-692*
respond-via-unicast	Sends a DHCP offer and DHCP Ack as unicast messages	*page 13-693*
update	Controls the usage of the DDNS service	*page 13-695*
static-binding	Configures static address bindings	*page 13-696*

address

dhcp-pool-mode commands

Adds a range of addresses to the DHCP pool. This is the range of IP addresses assigned to each device that joins the network.

Supported in the following platforms:

- Access Points — Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
address [<IP>|range <START-IP> <END-IP>] {class <DHCP-CLASS-NAME>}
```

Parameters

```
address [<IP>|range <START-IP> <END-IP>] {class <DHCP-CLASS-NAME>}
```

<IP>	Adds a single IP address to the DHCP pool
range <START-IP> <END-IP>	Adds a range of IP addresses to the DHCP pool • <START-IP> – Specify the first IP address in the range. • <END-IP> – Specify the last IP address in the range.
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

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#address 1.2.3.4 class
dhcpclass1

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#show context
 dhcp-pool pool1
  address 1.2.3.4 class dhcpclass1
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#
```

Related Commands:

no	Removes the DHCP pool's configured IP addresses
dhcp-class	Creates and configures the DHCP class parameters

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 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
bootfile <IMAGE-FILE-PATH>
```

Parameters

```
bootfile <IMAGE-FILE-PATH>
```

<IMAGE-FILE-PATH>	Sets the path to the boot image for the 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)#bootfile test.txt

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#show context
 dhcp-pool pool1
  address 1.2.3.4 class dhcpclass1
  bootfile test.txt
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#
```

Related Commands:

no	Resets the boot image path for the BOOTP clients
bootp	Configures the BOOTP protocol parameters

ddns

dhcp-pool-mode commands

Configures *Dynamic DNS* (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 configuration, the IP address of a device changes periodically. To enable the device to be accessible, its current IP address has to be published to a server that can resolve 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 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
ddns [domainname|multiple-user-class|server|ttl]

ddns domainname <DDNS-DOMAIN-NAME>
ddns multiple-user-class
ddns server <DDNS-SERVER-1> {<DDNS-SERVER-2>}
ddns ttl <1-864000>
```

Parameters

`ddns domainname <DDNS-DOMAIN-NAME>`

domainname <DDNS-DOMAIN-NAME>	Sets the domain name

`ddns multiple-user-class`

multiple-user-class	Enables the use of multiple user class with this DDNS domain

`ddns server <DDNS-SERVER-1> {<DDNS-SERVER-2>}`

server	Configures the DDNS server used by this DHCP profile
<ddns-server-1>	Configures the primary DDNS server. This is the default server.
<ddns-server-2>	Optional. Configures the secondary DDNS server. If the primary server is not reachable, this server is used.

`ddns ttl <1-86400>`

ttl <1-864000>	Configures the *Time To Live* (TTL) value for DDNS updates • <1-86400> – Specify a value from 1- 86400 seconds.

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#ddns domainname WID
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#ddns multiple-user-class
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#ddns server 172.16.10.9
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#show context
 dhcp-pool pool1
  address 1.2.3.4 class dhcpclass1
  ddns server 172.16.10.9
  ddns domainname WID
  ddns multiple-user-class
  bootfile test.txt
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#
```

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

Supported in the following platforms:

- Access Points — Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
default-router <IP> {<IP1>}
```

Parameters

```
default-router <IP> {<IP1>}
```

<IP>	Configures the primary router for a network
<IP1>	Optional. Configures the secondary router for a network. If the primary router is not available, this router is used.

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)#default-router 172.16.10.8
172.16.10.9

rrfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#show context
 dhcp-pool pool1
  address 1.2.3.4 class dhcpclass1
  ddns server 172.16.10.9
  ddns domainname WID
  ddns multiple-user-class
  bootfile test.txt
  default-router 172.16.10.8 172.16.10.9
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#
```

Related Commands:

no	Removes 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 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
dns-server <IP> {<IP1>}
```

Parameters

```
dns-server <IP> {<IP1>}
```

<IP>	Configures the primary DNS server's IP address • <IP> – Sets the server's IP address. Up to 8 IPs can be set
<IP1>	Optional. Configures the secondary DNS server's IP address. If the primary server is not available, this server is used.

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#dns-server 172.16.10.7

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#show context
 dhcp-pool pool1
  address 1.2.3.4 class dhcpclass1
  ddns server 172.16.10.9
  ddns domainname WID
  ddns multiple-user-class
  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)#
```

Related Commands:

no	Removes DNS server settings

domain-name

dhcp-pool-mode commands

Sets the domain name for the DHCP pool

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 6511 Access Point, Brocade Mobility 71XX 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>	Defines the DHCP pool's domain name

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#domain-name documentation

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#show context
 dhcp-pool pool1
```

```
  address 1.2.3.4 class dhcpclass1
  ddns server 172.16.10.9
  ddns domainname WID
  ddns multiple-user-class
  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)#
```

Related Commands:

no	Removes a DHCP pool's domain name

excluded-address

dhcp-pool-mode commands

Prevents a DHCP server from assigning certain addresses in the DHCP pool

Supported in the following platforms:

- Access Points — Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
excluded-address [<IP>|range]

excluded-address <IP>
excluded-address range <START-IP> <END-IP>
```

Parameters

```
excluded-address <IP>
```

<IP>	Excludes a single IP address in the DHCP pool

```
excluded-address range <START-IP> <END-IP>
```

range <START-IP> <END-IP>	Excludes a range of IP addresses in the DHCP pool

Example

```
rfs7000-37FABE(config-dhcp-policy-test)#excluded-address range 172.16.10.9
172.16.10.10

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#show context
 dhcp-pool pool1
  address 1.2.3.4 class dhcpclass1
  ddns server 172.16.10.9
  ddns domainname WID
  ddns multiple-user-class
  excluded-address range 172.16.10.9 172.16.10.10
  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)#
```

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 for a DHCP client. Once this 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. The lease period is about 24 hours.

Supported in the following platforms:

- Access Points — Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 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

```
rfs7000-37FABE(config-dhcp-policy-test-pool-test)#lease 100 23 59 59

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#show context
 dhcp-pool pool1
  address 1.2.3.4 class dhcpclass1
  lease 100 23 59 59
  ddns server 172.16.10.9
  ddns domainname WID
  ddns multiple-user-class
  excluded-address range 172.16.10.9 172.16.10.10
  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)#
```

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 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
netbios-name-server <IP> {<IP1>}
```

Parameters

```
netbios-name-server <IP> {<IP1>}
```

<IP>	Configures primary NetBIOS server's IP address for a DHCP pool
<IP1>	Configures secondary NetBIOS server's IP address

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#netbios-name-server
172.16.10.23

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#show context
 dhcp-pool pool1
  address 1.2.3.4 class dhcpclass1
  lease 100 23 59 59
  ddns server 172.16.10.9
  ddns domainname WID
  ddns multiple-user-class
  excluded-address range 172.16.10.9 172.16.10.10
  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)#
```

Related Commands:

no	Removes the NetBIOS 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 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 type as broadcast node • h-node – Sets the type as hybrid node • m-node – Sets the type as mixed node • p-node – Sets the type as peer-to-peer node

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#netbios-node-type b-node

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#show context
 dhcp-pool pool1
  address 1.2.3.4 class dhcpclass1
  lease 100 23 59 59
  ddns server 172.16.10.9
  ddns domainname WID
  ddns multiple-user-class
  excluded-address range 172.16.10.9 172.16.10.10
  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)#
```

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 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
network <IP/M>
```

Parameters

```
network <IP/M>
```

<IP/M>	Configures the network number and mask (for example, 192.168.0.0/24)

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#network 172.16.0.0/24

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#show context
 dhcp-pool pool1
  network 172.16.0.0/24
  address 1.2.3.4 class dhcpclass1
  lease 100 23 59 59
  ddns server 172.16.10.9
  ddns domainname WID
  ddns multiple-user-class
  excluded-address range 172.16.10.9 172.16.10.10
  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)#
```

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 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
next-server <IP>
```

Parameters

```
next-server <IP>
```

<IP>	Configures the IP address of the next server in the boot process

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#next-server 172.16.10.24

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#show context
```

```
 dhcp-pool pool1
  network 172.16.0.0/24
  address 1.2.3.4 class dhcpclass1
  lease 100 23 59 59
  ddns server 172.16.10.9
  ddns domainname WID
  ddns multiple-user-class
  excluded-address range 172.16.10.9 172.16.10.10
  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)#
```

Related Commands:

no	Removes the next server configuration settings

no

dhcp-pool-mode commands

Negates a command or sets its default

Supported in the following platforms:

- Access Points — Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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>|all]
no address range <START-IP> <END-IP>

no ddns [domainname|multiple-user-class|server|ttl]

no excluded-address <IP>
no excluded-address range <START-IP> <END-IP>

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>|all]
```

no address	Resets configured DHCP pool addresses
<IP>	Removes an IP address from the list of addresses
all	Removes configured DHCP IP addresses

```
no address range <START-IP> <END-IP>
```

no address	Resets the DHCP pool addresses
range <START-IP> <END-IP>	Removes a range of IP address from the list of addresses • <START-IP> – Specify the first IP address in the range. • <END-IP> – Specify the last IP address in the range.

```
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>
```

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.

```
no excluded-address range <START-IP> <END-IP>
```

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> <END-IP>	Specifies the IP address range • <START-IP> – Specify the first IP address in the range. • <END-IP> – Specify the last IP address in the range.

`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:

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#show context
 dhcp-pool pool1
  network 172.16.0.0/24
  address 1.2.3.4 class dhcpclass1
  lease 100 23 59 59
  ddns server 172.16.10.9
  ddns domainname WID
  ddns multiple-user-class
  excluded-address range 172.16.10.9 172.16.10.10
  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)#

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#no bootfile
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#no network
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#no default-router
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#no next-server
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#no domain-name
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#no excluded-address range
172.16.10.9 172.16.10.10
```

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#no ddns domainname
rfs7000-37FABE(config-dhcp-policy-test-pool-test)#no lease

The following example shows the DHCP pool settings after the ‘no’ commands are
executed:

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#show context
 dhcp-pool pool1
  address 1.2.3.4 class dhcpclass1
  ddns server 172.16.10.9
  ddns multiple-user-class
  netbios-node-type b-node
  dns-server 172.16.10.7
  netbios-name-server 172.16.10.23
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#
```

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 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

Usage Guidelines:

Defines non standard DHCP option codes (0-254)

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

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#option option1
157.235.208.80

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#show context
 dhcp-pool pool1
  address 1.2.3.4 class dhcpclass1
  ddns server 172.16.10.9
  ddns multiple-user-class
  netbios-node-type b-node
  dns-server 172.16.10.7
  netbios-name-server 172.16.10.23
  option option1 157.235.208.80
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#
```

Related Commands:

no	Resets values or disables the DHCP pool option settings

respond-via-unicast

dhcp-pool-mode commands

Sends a DHCP offer and a DHCP Ack as unicast messages

Supported in the following platforms:

- Access Points — Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
respond-via-unicast
```

Parameters

None

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#respond-via-unicast

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#show context
 dhcp-pool pool1
  address 1.2.3.4 class dhcpclass1
  ddns server 172.16.10.9
  ddns multiple-user-class
  netbios-node-type b-node
  dns-server 172.16.10.7
  netbios-name-server 172.16.10.23
  option option1 157.235.208.80
  respond-via-unicast
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#
```

Related Commands:

no	Disables sending of a DHCP offer and DHCP Ack as unicast 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 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#static-route 1.2.3.4/8
5.6.7.8

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#show context
 dhcp-pool pool1
  address 1.2.3.4 class dhcpclass1
  ddns server 172.16.10.9
  ddns multiple-user-class
  netbios-node-type b-node
  dns-server 172.16.10.7
```

```
  netbios-name-server 172.16.10.23
  option option1 157.235.208.80
  respond-via-unicast
  static-route 1.2.3.4/8 5.6.7.8
  static-binding client-identifier test
  static-binding hardware-address 11-22-33-44-55-66
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#
```

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 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
update dns {override}
```

Parameters

```
update dns {override}
```

dns {override}	Configures the DDNS parameters • override – Optional. Enables DDNS updates on a onboard DHCP server

Usage Guidelines:

A DHCP client cannot perform updates for RR's A, TXT and PTR. 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

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#update dns override

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#show context
 dhcp-pool pool1
  address 1.2.3.4 class dhcpclass1
  update dns override
  ddns server 172.16.10.9
  ddns multiple-user-class
  netbios-node-type b-node
  dns-server 172.16.10.7
  netbios-name-server 172.16.10.23
  option option1 157.235.208.80
  respond-via-unicast
  static-route 1.2.3.4/8 5.6.7.8
  static-binding client-identifier test
```

```
  static-binding hardware-address 11-22-33-44-55-66
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#
```

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.

Table 46 summarizes static binding configuration commands.

TABLE 46 Static-Binding-Config Commands

Command	Description	Reference
static-binding	Creates a static binding policy and enters its configuration mode	*page 13-696*
static-binding-mode commands	Invokes static binding configuration commands	*page 13-698*

static-binding

static-binding

Configures static address bindings

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

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#static-binding
client-identifier test
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-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

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-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 commands
static-binding	Describes the static binding mode commands

static-binding-mode commands

static-binding

Table 47 summarizes static binding configuration commands.

TABLE 47 Static-Binding-Config-Mode Commands

Command	Description	Reference
bootfile	Assigns a Bootfile name for the DHCP configuration on the network pool	*page 13-698*
client-name	Configures a client name	*page 13-699*
default-router	Configures default router or gateway IP address	*page 13-699*
dns-server	Sets the DNS server's IP address available to all DHCP clients connected to the DHCP pool	*page 13-700*
domain-name	Sets the network pool's domain name	*page 13-701*
ip-address	Configures a host's fixed IP address	*page 13-702*
netbios-name-server	Configures a NetBIOS (WINS) name server IP address	*page 13-702*
netbios-node-type	Defines the NetBIOS node type	*page 13-703*
next-server	Specifies the next server used in the boot process	*page 13-704*
no	Negates a command or sets its default	*page 13-705*
option	Configures raw DHCP options	*page 13-707*
respond-via-unicast	Sends a DHCP offer and DHCP Ack as unicast messages	*page 13-707*
static-route	Adds static routes installed on DHCP clients	*page 13-708*

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 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 commands
bootp	Configures BOOTP protocol parameters

client-name

static-binding-mode commands

Specifies a name for a client

Supported in the following platforms:

- Access Points — Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
client-name <NAME>
```

Parameters

```
client-name <NAME>
```

<NAME>	Specify the client name where this static binding policy is applied

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 commands

default-router

dhcp-pool-mode commands

Configures a default router or gateway IP address for the static binding configuration

Supported in the following platforms:

- Access Points — Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
default-router <IP> {<IP1>}
```

Parameters

```
default-router <IP> {<IP1>}
```

<IP>	Configures the primary network router
<IP1>	Optional. Configures the secondary network router. If the primary router is not available, this router is used.

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 commands

dns-server

dhcp-pool-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 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
dns-server <IP> {<IP1>}
```

Parameters

```
dns-server <IP> {<IP1>}
```

<IP>	Configures the primary DNS server's IP address • <IP> – Sets the server's IP address (up to 8 IPs can be set)
<IP1>	Optional. Configures the secondary DNS server's IP address

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 commands

domain-name

dhcp-pool-mode commands

Sets the domain name for the static binding configuration

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 6511 Access Point, Brocade Mobility 71XX 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>	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 commands

ip-address

static-binding-mode commands

Configures a fixed IP address for a host

Supported in the following platforms:

- Access Points — Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
ip-address <IP>
```

Parameters

```
ip-address <IP>
```

<IP>	Configures a fixed host IP address in dotted decimal format

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 commands

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 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
netbios-name-server <IP> {<IP1>}
```

Parameters

```
netbios-name-server <IP> {<IP1>}
```

<IP>	Configures the primary NetBIOS server's IP address
<IP1>	Optional. Configures the secondary NetBIOS server's IP address

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 commands

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 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 broadcast node • h-node – Sets the hybrid node • m-node – Sets the mixed node • p-node – Sets the peer-to-peer node

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 commands

next-server

static-binding-mode commands

Configures the next server utilized in the boot process

Supported in the following platforms:

- Access Points — Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
next-server <IP>
```

Parameters

```
next-server <IP>
```

<IP>	Configures the IP address of the next server in the boot process

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 commands

no

dhcp-pool-mode commands

Negates a command or sets its default for the static binding commands

Supported in the following platforms:

- Access Points — Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 [bootfile|client-name|default-router|dns-server|domain-name|ip-address|

netbios-name-server|netbios-node-type|next-server|respond-via-unicast]

no option <OPTION-NAME>

no static-route <IP/MASK> <GATEWAY-IP>
```

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 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 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 6511 Access Point, Brocade Mobility 71XX Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 commands

static-route

static-binding-mode commands

Adds static routes to the static binding configuration

Supported in the following platforms:

- Access Points — Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 commands

no

dhcp-server-policy

Negates a command or sets its default

Supported in the following platforms:

- Access Points — Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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-pool-mode commands

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 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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	Resets values or disables commands

ping

dhcp-server-policy

Specifies DHCP server ping parameters

Supported in the following platforms:

- Access Points — Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
ping timeout <1-10>
```

Parameters

```
ping timeout <1-10>
```

timeout <1-10>	Sets the ping timeout from 1 - 10 seconds

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 values or disables commands

Chapter

Firewall-Policy

14

In this chapter

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:

```
RFSSwitch(config)#firewall-policy <POLICY-NAME>

rfs7000-37FABE(config)#firewall-policy test
rfs7000-37FABE(config-fw-policy-test)#?
Firewall policy Mode commands:
  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 48 summarizes default firewall policy configuration commands.

TABLE 48 Firewall-Policy-Config Commands

Command	Description	Reference
alg	Enables an algorithm	*page 14-715*
clamp	Sets a clamp value to limit TCP MSS to inner path-MTU for tunnelled packets	*page 14-715*
dhcp-offer-convert	Enables the conversion of broadcast DHCP offers to unicast	*page 14-716*
dns-snoop	Sets the timeout value for DNS entries	*page 14-716*
firewall	Configures the wireless firewall	*page 14-717*
flow	Defines a session flow timeout	*page 14-718*
ip	Sets an IP address for a selected device	*page 14-719*
ip-mac	Defines an action based on IP-MAC table	*page 14-724*
logging	Enables enhanced firewall logging	*page 14-726*
no	Negates a command or reverts settings to their default	*page 14-727*
proxy-arp	Enables the generation of ARP responses on behalf of another device	*page 14-734*
stateful-packet-inspection-12	Enables stateful packets-inspection in layer 2 firewall	*page 14-734*
storm-control	Defines storm control and logging settings	*page 14-735*
virtual-defragmentation	Enables virtual defragmentation for IPv4 packets	*page 14-736*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
do	Runs commands from the EXEC mode	*page 4-165*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes information to the memory or terminal	*page 5-310*

alg

firewall-policy

Enables preconfigured algorithms supporting a particular protocol

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
alg [dns|facetime|ftp|sccp|sip|tftp]
```

Parameters

```
alg [dns|facetime|ftp|sccp|sip|tftp]
```

alg	Enables preconfigured algorithms
dns	Enables the *Domain Name System* (DNS) algorithm
facetime	Enables the FaceTime algorithm
ftp	Enables the *File Transfer Protocol* (FTP) algorithm
sccp	Enables the *Skinny Call Control Protocol* (SCCP) algorithm
sip	Enables the *Session Initiation Protocol* (SIP) algorithm
tftp	Enables the *Trivial File Transfer Protocol* (TFTP) algorithm

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 ramains in the DNS snoop table only for the specified time, and is deleted once this time is exceeded.

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

```
flow timeout [icmp|other] <1-32400>
```

timeout	Configures a packet timeout
icmp	Configures the timeout for ICMP packets
other	Configures the timeout for packets that are not ICPM, TCP, or UDP
<1-32400>	Configures the timeout interval from 1 - 32400 seconds

```
flow timeout udp <15-32400>
```

timeout	Configures a packet timeout
udp	Configures the timeout for UDP packets
<15-32400>	Configures the timeout interval 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
reset	Configures the reset TCP flow timeout interval
setup	Configures the opening TCP flow timeout interval
stateless-fin-or-reset	Configures stateless TCP flow timeout created with the FIN or RESET packets
stateless-general	Configures the stateless TCP flow timeout
<1-32400>	Configures the timeout interval 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 interval
<15-32400>	Configures the timeout interval 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 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 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}
          [log-and-drop|log-only] log-level
[<0-7>|alerts|critical|debugging|emergencies|
          errors|informational|notifications|warnigns]

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 <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-solicit|smurf|snork
|
tcp-bad-sequence|tcp-fin-scan|tcp-intercept|tcp-null-scan|tcp-post-scan|tcp-s
```

equence-past-window|*tcp-xmas-scan*|*tcphdrfrag*|*twinge*|*udp-short-hdr*|*winnuke*}
[log-and-drop|log-only] log-level
[<0-7>|alerts|critical|debug|emergencies|errors|informational|
notifications|warnigns]

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.
broadcast-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 an 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 the 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. In this attack, 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 TPC 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 TCP post SYN DoS attacks
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
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-pos
t-scan|
tcp-sequence-past-window|tcp-xmas-scan|tcphdrfrag|twinge|udp-short-hdr|winnuk
e}
[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 TPC 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)
<472-1460>	Sets the TCP MSS value from 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]
```

tcp	Identifies and configures TCP events and configuration items
optimize-unnecessary-resends	Enables the validation of unnecessary of 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 acknowledgement 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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
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
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
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

`ip-mac routing conflict drop-only`

routing	Defines a routing table based action
conflict	Action performed when a conflict exists in the routing table
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
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 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

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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
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
malformed-packet-drop	Drops raw IP packets that do not pass sanity checks
all	Logs all messages
rate-limited	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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
no [alg|clamp|dhcp-offer-convert|dns-snoop|firewall|flow|ip|ip-mac|logging|

proxy-arp|stateful-packet-inspection-l2|storm-control|virtual-defragmentation
]

no [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-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 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 [dhcp-offer-convert|proxy-arp|stateful-packet-inspection-l2]
```

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 limiting the TCP MSS size 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 following packet types:
icmp	Disables ICMP packet timeout
others	Disables the timeout for packets that are not 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 the following 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 TPC 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 acknowledgement 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 or 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
```

Related Commands:

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

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

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.

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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
maximum-fragments-per-datagram <2-8129>	Optional. Defines the maximum IPv4 fragments per datagram • <2-8129> – Sets a value from 2 - 8129
minimum-first-fragment-length <8-1500>	Optional. Defines the minimum length required for the first IPv4 fragment • <8-1500> – Sets a value from 8 - 1500

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

14

Chapter

15

Mint-Policy

In this chapter

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 MiNT policy instance, use the following commands:

```
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
  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 49 summarizes MiNT policy configuration commands.

TABLE 49 MiNT-Policy-Config Commands

Command	Description	Reference
level	Configures the MiNT routing level	*page 15-740*
mtu	Configures the global MiNT MTU	*page 15-741*
no	Negates a command or sets its default	*page 15-742*
udp	Configures the MiNT UDP/IP encapsulation parameters	*page 15-741*

TABLE 49 MiNT-Policy-Config Commands

Command	Description	Reference
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
do	Runs commands from the EXEC mode	*page 4-165*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-165*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes information to the memory or terminal	*page 5-310*

level

mint-policy

Configures the global MiNT routing level

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 • <1-1677215> – Specify a value from 1 - 16777215.

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. The higher the MTU values, the greater 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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.

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 Negates the configured maximum packet size for MiNT routing

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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. The specified value becomes the default UDP port. The value must be an even number, since data packets use the control port +1.

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, and UDP or IP encapsulation settings.

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
no [level|mtu|udp]

no level 2 area-id

no mtu

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 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
udp	Configures the MiNT UDP/IP encapsulation parameters

15

Chapter

Management-Policy

16

In this chapter

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.

Use the (config) instance to configure management policy related configuration commands. To navigate to the config management policy instance, use the following commands:

```
rfs7000-37FABE(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 brocade
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 (UI
                        or mapsh)
  no                    Negate a command or set its defaults
  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)#
```

16

management-policy

Table 50 summarizes management policy configuration commands.

TABLE 50 Management-Policy-Config Commands

Command	Description	Reference
aaa-login	Sets login authentication settings	*page 16-746*
banner	Defines a login banner name	*page 16-748*
ftp	Enables a FTP server	*page 16-748*
http	Enables a HTTP server	*page 16-750*
https	Enables a secure HTTPS server	*page 16-750*
idle-session-timeout	Sets the interval after which a session is terminated	*page 16-751*
no	Negates a command or sets its default	*page 16-752*
restrict-access	Restricts management access to a set of hosts or subnets	*page 16-755*
snmp-server	Sets the SNMP server parameters	*page 16-757*
ssh	Enables SSH	*page 16-760*
telnet	Enables Telnet	*page 16-761*
user	Creates a new user account	*page 16-762*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 16-763*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
do	Runs commands from the EXEC mode	*page 4-165*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-165*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes information to the memory or terminal	*page 5-310*

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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
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.

`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.

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 login banner message. Use this command to display messages to users as they as login.

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
banner motd <LINE>
```

Parameters

```
banner motd <LINE>
```

motd <LINE>	Sets the *message of the day* (motd) banner • <LINE> – Defines the message string

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

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 • <ENCRYPTED-PASSWORD> – Specify the password.
<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.

`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.
[password 1 <ENCRYPTED-PASSWORD>]]	Configures an encrypted password • <ENCRYPTED-PASSWORD> – Specifies an encrypted password (use this option if copy pasting from another device)
<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
example@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 the *Hyper Text Transport Protocol* (HTTP) server on this management policy

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
http server
```

Parameters

```
http server
```

http server	Enables the HTTP server on this management policy

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 the HTTP server on this management policy

https

management-policy

Enables the secure *Hyper Text Transport Protocol Secure* (HTTPS) server on this management policy

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
https server
```

Parameters

```
https server
```

https server	Enables the HTTPS server on this management policy

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 the HTTPS server on this management policy

idle-session-timeout

management-policy

Configures a session's idle timeout. After the timeout interval is exceeded, the session is automatically terminated.

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
idle-session-timeout <0-1440>
```

Parameters

```
idle-session-timeout <0-1440>
```

<0-1440>	Sets the interval, in minutes, after which a configuration session is timed out. Specify a value from 0 - 1440 minutes. Zero (0) indicates the session is never terminated.

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	Disables an idle session timeout

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 parameters.

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
no [aaa-login|banner|ftp|http|https|idle-session-timeout|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|restrict-access]
```

```
no snmp-server
[community|enable|host|manager|max-pending-requests|request-timeout|
          return-security-configuration|throttle|user]

no snmp-server [community <WORD>|display-vlan-info-per-radio|enable traps|
          host <IP> {<1-65535>}|manager
[all|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|restrict-access]`

no idle-session-timeout	Disables a defined session timeout interval
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|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 sending SNMP traps to default (162)
manager [all|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
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

restrict-access

management-policy

Restricts management access to a set of hosts or subnets

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
restrict-access [host|ip-access-list|subnet]

restrict-access host <IP> {log|subnet}
restrict-access host <IP> {log [all|denied-only]}
restrict-access host <IP> {subnet <IP/M> {log [all|denied-only]}}

restrict-access ip-access-list <IP-ACCESS-LIST-NAME>

restrict-access subnet <IP/M> {host|log}
restrict-access subnet <IP/M> {log [all|denied-only]}
restrict-access subnet <IP/M> {host <IP> {log [all|denied-only]}}
```

Parameters

`restrict-access host <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.
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

`restrict-access host <IP> {subnet <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 IP address.
subnet <IP/M>	Optional. Restricts access 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
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

`restrict-access ip-access-list <IP-ACCESS-LIST-NAME>`

ip-access-list	Uses an IP access list to filter access requests
<IP-ACCESS-LIST-NAME>	Sets the access list name

`restrict-access subnet <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
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

```
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

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 parameters

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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|v2|v3]|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 • rw – Assigns read and write access to the specified SNMP community

`snmp-server enable traps`

enable traps	Enables SNMP traps sent to the management stations. Enabling this feature ensures the despatch of SNMP notifications to all hosts.

`snmp-server host <IP> [v2c|v3] {<1-65535>}`

host <IP>	Configures a host's IP address
[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 • <1-65535> – Optional. Sets a value from 1 - 65535. The default port is 162.

`snmp-server [manager [all|v2|v3]|max-pending-requests {<64-1024>}| request-timeout {<2-720>}]`

manager [all|v2|v3]	Enables SNMP manager and specifies the SNMP version • all – Enables SNMP manager version v2 and v3 • v2 – Enables SNMP manager version v2 only • v3 – Enables SNMP manager version v3 only
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 the 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 example1123

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 example1123
 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 SSH for this management policy. SSH encrypts communication between the client and the server.

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 • <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 example1123
 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. By default Telnet is enabled on *Transmission Control Protocol* (TCP) port 23. Use this command to change the TCP port.

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
telnet {port <1-65535>}
```

Parameters

```
telnet {port <1-65535>}
```

telnet	Enables Telnet
port <1-65535>	Optional. Configures the Telnet port • <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 example1123
 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

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 • 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 example1123
 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 crashfiles in flash:/crashinfo
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 an update of CLI prompt settings

Chapter

Radius-Policy 17

In this chapter

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-server-policy*
- *radius-user-pool-policy*

radius-group

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 *Remote Authentication Dial-in user Service* (RADIUS) group. To navigate to the RADIUS group instance, use the following commands:

```
rfs7000-37FABE(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 51 summarizes RADIUS group configuration commands.

TABLE 51 RADIUS-Group-Config Commands

Command	Description	Reference
guest	Enables guest access for the newly created group	*page 17-767*
no	Negates a command or reverts settings to their default	*page 17-771*
policy	Configures RADIUS group access policy parameters	*page 17-768*
rate-limit	Sets the default rate limit per user in Kbps, and applies it to all enabled WLANs	*page 17-770*
clrscr	Clears the display screen	*page 5-275*

TABLE 51 RADIUS-Group-Config Commands

Command	Description	Reference
commit	Commits (saves) changes made in the current session	*page 5-276*
do	Runs commands from the EXEC mode	*page 4-165*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes information to memory or terminal	*page 5-310*

guest

radius-group

Configures this group as a guest (non-management) group. A guest user group has temporary permissions to the local RADIUS server. You can configure multiple guest user groups, each having a unique set of RADIUS policy 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 300 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers – Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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	Creates 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 300 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers – Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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|
super-user|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 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).

`policy access [all|console|ssh|telnet|web] {(all|console|ssh|telnet|web)}`

access	Configures a group access type • 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|super-user|system-admin|web-user-admin]`
role [helpdesk|monitor|network-admin|security-admin|super-user|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 • 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.
	`policy ssid <SSID>`
ssid <SSID>	Sets the *Service Set Identifier* (SSID) for this RADIUS 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 RADIUS group members can access the local RADIUS resources. The options are. • 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 These parameters are recursive and you can provide access on multiple days.
	`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 role
- 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 example

rfs7000-37FABE(config-radius-group-test)#show context
radius-group test
 guest
 policy vlan 1
 policy ssid example
 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 RADIUS server group

Supported in the following platforms:

- Access Points – Brocade Mobility 300 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers – Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 A value of 0 disables rate limiting.
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 A value of 0 disables rate limiting.

Usage Guidelines:

Use `[no] rate-limit [wired-to-wireless|wireless-to-wired]`to remove the rate limit applied to the group.

`[no] rate-limit [wireless-to-wired]`sets the rate limit back to unlimited

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 example
 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 non-management 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 300 Access Point, Brocade Mobility 71XX Access Point

- Wireless Controllers – Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 group

`no policy access [all|console|ssh|telnet|web]`

no policy access	Removes or modifies the RADIUS 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 this RADIUS 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 • 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 the RADIUS group's SSID • <SSID> – Specify the RADIUS group SSID • all – Removes all allowed WLANs

`no policy [role|time|vlan]`

no policy role	Removes the RADIUS group's role
no policy time	Removes the RADIUS group's start and end access time
no policy vlan	Removes the RADIUS group's VLAN ID

```
no rate-limit [from-air|to-air]
```

no rate-limit	Removes RADIUS group's rate limit
from-air	Removes the rate limit in the uplink direction, from the wireless client to the network
to-air	Sets the rate limit in the downlink direction, from the network to the wireless client

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 example
 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 example
 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

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 ensures the information is correct using authentication schemes like PAP, CHAP or EAP. 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 LDAP resource to verify the 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:

```
rfs7000-37FABE(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-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)#
```

Table 52 summarizes RADIUS server policy configuration commands.

TABLE 52 RADIUS-Server-Policy-Config Commands

Commands	Description	Reference
authentication	Configures the RADIUS authentication parameters	*page 17-775*
chase-referral	Enables LDAP server referral chasing	*page 17-776*
crl-check	Enables a *certificate revocation list* (CRL) check	*page 17-777*
ldap-group-verification	Enables the LDAP group verification settings	*page 17-777*
ldap-server	Configures the LDAP server parameters	*page 17-778*
local	Configures a local RADIUS realm	*page 17-780*

TABLE 52 RADIUS-Server-Policy-Config Commands

Commands	Description	Reference
nas	Configures the key sent to a RADIUS client	*page 17-781*
no	Negates a command or sets its defaults	*page 17-782*
proxy	Configures the RADIUS proxy server settings	*page 17-784*
session-resumption	Enables session resumption	*page 17-786*
use	Defines settings used with the RADIUS server policy	*page 17-787*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in this current session	*page 5-276*
do	Runs commands in the EXEC mode	*page 4-165*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to the their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug (config-if) instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes information to the memory or terminal	*page 5-310*

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 300 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers – Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
authentication [data-source|eap-auth-type]
authentication data-source [ldap {fallback}|local]
authentication eap-auth-type [all|peap-gtc|peap-mschapv2|tls|ttls-md5|
          ttls-mschapv2|ttls-pap]
```

Parameters

```
authentication data-source [ldap {fallback}|local]
```

data-source	The RADIUS sever uses multiple data sources to authenticate a user. It is necessary to specify the data source. The options are: LDAP and local The default setting is local.

ldap fallback	Uses a remote *Lightweight Directory Access Protocol* (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.
local	Uses the local user database to authenticate a user

```
authentication eap-auth-type [all|peap-gtc|peap-mschapv2|tls|ttls-md5|
ttls-mschapv2|ttls-pap]
```

data-source	The RADIUS sever uses multiple data sources to authenticate a user. It is necessary to specify the data source. The options are: LDAP and local The default setting is local.
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 GTC
peap-mschapv2	Enables PEAP with default MSCHAPv2
tls	Enables TLS
ttls-md5	Enables TTLS with default md5
ttls-mschapv2	Enables TTLS with default MSCHAPv2
ttls-pap	Enables TTLS with default 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 LDAP server referral chasing. Chase referral allows a domain controller to refer a client application to another domain controller that may contain the requested object. The referred domain controller may generate a second referral, if it too does not contain the requested object.

Supported in the following platforms:

- Access Points – Brocade Mobility 300 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers – Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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.

Supported in the following platforms:

- Access Points – Brocade Mobility 300 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers – Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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-group-verification

radius-server-policy

Enables LDAP group verification settings on this RADIUS server policy

Supported in the following platforms:

- Access Points – Brocade Mobility 300 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers – Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 parameters. 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 300 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers – Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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. 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> – Sets the LDAP server's IP address
port <1-65535>	Configures the LDAP server port • <1-65535> – Sets a port between 1 - 65535
login <LOGIN-NAME>	Configures the login name of a user to access the LDAP server • <LOGIN-ID> – Sets 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>	Select a value from 1 - 10 to configure the network timeout (number of seconds to wait for a response from the server)

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 example bind-dn bind-dn1 base-dn base-dn1 passwd 0 moto
rolasol@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 "example" bind-dn
"bind-dn1" base-dn "base-dn1" passwd 0 example@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 300 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers – Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 "example" bind-dn
"bind-dn1" base-dn "base-dn1" passwd 0 example@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

Supported in the following platforms:

- Access Points – Brocade Mobility 300 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers – Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 32 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 "example" bind-dn
"bind-dn1" base-dn "base-dn1" passwd 0 example@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 300 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers – Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
no
[authentication|chase-referral|clr-check|ldap-group-verification|ldap-server|
local|
          nas|proxy|session-resumption|use]

no authentication [data-source {ldap {fallback}|local}|eap configuration]

no [chase-referral|clr-check|ldap-group-verification|nas
<IP/M>|session-resumption]

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}	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
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	
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 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-GROU-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 "example" bind-dn
"bind-dn1" base-dn "bas-dn1" passwd 0 example@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 "example" bind-dn
"bind-dn1" base-dn "bas-dn1" passwd 0 example@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-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 300 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers – Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 • <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 wireless 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 example1123

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 example1123
 ldap-server primary host 172.16.10.19 port 162 login "example" bind-dn
"bind-dn1" base-dn "bas-dn1" passwd 0 example@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.

Supported in the following platforms:

- Access Points – Brocade Mobility 300 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers – Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 example1123
 ldap-server primary host 172.16.10.19 port 162 login "example" bind-dn
"bind-dn1" base-dn "bas-dn1" passwd 0 example@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 300 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers – Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 example1123
 ldap-server primary host 172.16.10.19 port 162 login "example" bind-dn
"bind-dn1" base-dn "bas-dn1" passwd 0 example@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

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:

```
rfs7000-37FABE(config)#radius-user-pool-policy <POOL-NAME>
rfs7000-37FABE(config)#radius-user-pool-policy testuser
rfs7000-37FABE(config-radius-user-pool-testuser)#
```

Table 53 summarizes RADIUS user pool policy configuration commands.

TABLE 53 RADIUS-User-Pool-Policy-Config Commands

Commands	Description	Reference
user	Configures the RADIUS user parameters	*page 17-790*
no	Negates a command or sets its default	*page 17-790*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*

TABLE 53 RADIUS-User-Pool-Policy-Config Commands

Commands	Description	Reference
do	Runs commands from the EXEC mode	*page 4-165*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug (config-if) instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes information to the memory or terminal	*page 5-310*

user

radius-user-pool-policy

Configures RADIUS user parameters

Supported in the following platforms:

- Access Points – Brocade Mobility 300 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers – Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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:YYY>
          {(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. 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.
guest	Optional. Enables guest user 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. 12:15:2012).
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>| satrt-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
motoro
lasol@123 group test1 guest expiry-time 13:20 expiry-date 12:25:2012
start-time
17:00 start-date 01:05:2012
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 example@123 group test1 guest expiry-time 13:20
expiry-date 12:25:2012 start-time 17:00 start-date 01:05:2012
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 300 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers – Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 example@123 group test1 guest expiry-time 13:20
expiry-date 12:25:2012 start-time 17:00 start-date 01:05:2012
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

17

Chapter

Radio-QOS-Policy

18

In this chapter

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 the 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 the 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 wireless controllers and access points include a *Session Initiation Protocol* (SIP), *Skinny Call Control Protocol* (SCCP) and *Application Layer Gateway* (ALGs) enabling devices to identify voice streams and dynamically set voice call bandwidth.

Brocade wireless controllers and access points 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:

```
rfs7000-37FABE(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 54 summarizes radio QoS policy configuration commands.

TABLE 54 Radio-QoS-Policy-Config Commands

Command	Description	Reference
accelerated-multicast	Configures multicast streams for acceleration	*page 18-795*
admission-control	Enables admission control across all radios for one or more access categories	*page 18-796*
no	Negates a command or resets configured settings to their default	*page 18-799*
smart-aggregation	Configures smart aggregation parameters	*page 18-801*
wmm	Configures 802.11e/wireless multimedia parameters	*page 18-802*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
do	Runs commands from the EXEC mode	*page 4-165*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes information to the memory or terminal	*page 5-310*

accelerated-multicast

radio-qos-policy

Configures multicast streams for acceleration. Multicasting allows the group transmission of data streams.

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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
stream-threshold <1-500>	Configures the number of packets per second threshold for streams to accelerate • <1-500> – Specify a value from 1 - 500. The default is 30.

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 *Application Layer Gateways* (ALG). For example, *Session Initiation Protocol* (SIP) voice calls. 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 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 • 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 • 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 • 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 • <0-150> – Specify a value from 0 - 150. This is the maximum percentage of airtime, including oversubscription, for this 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 • <0-256> – Specify a value from 0 - 256. This is the maximum number of wireless clients admitted to this 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 • <0-256> – Specify a value from 0 - 256. This is the maximum number of roaming wireless clients admitted to this 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. • <0-150> – Specify a value from 0 - 150. This is the percentage of air time, including oversubscription, allocated exclusively for roaming clients associated with this 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
no [accelerated-multicast|admission-control|smart-aggregation|wmm]

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 [background|best-effort|streaming-video|
          video-conferencing|voice]|min-aggregation-limit}

no wmm [background|best-effort|video|voice] [aifsn|cw-max|cw-min|txop-limit]
```

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 • max-client-streams – Resets the maximum number of accelerated streams per client to the default • max-streams – Resets the maximum number of accelerated streams to the default • overflow-policy – Resets the overflow policy to the default (reject) • stream-threshold – Resets the number of packets per second threshold to the default

`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 • best-effort – Resets best effort access category admission control • video – Resets video access category admission control • voice – Resets voice access category admission control
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]|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
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 – Resets background access category wireless multimedia settings • best-effort – Resets best effort access category wireless multimedia settings • video – Resets video access category wireless multimedia settings • voice – Resets voice access category wireless multimedia settings The following are common to the background, best-effort, video, and voice parameters:
aifsn	Resets *Arbitration Inter Frame Spacing Number* (AIFSN) to its default
cw-max	Resets the maximum contention window to its default
cw-min	Resets the minimum contention window to its default
txop-limit	Resets the transmit opportunity limit to its default

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)#
```

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
wmm	Configures 802.11e wireless multimedia parameters

smart-aggregation

radio-qos-policy

Configures smart aggregation parameters with this Radio QoS policy

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
smart-aggregation {delay|min-aggregation-limit}
smart-aggregation {delay
[background|best-effort|streaming-video|video-conferencing|
          voice] <0-1000>}
smart-aggregation min-aggregation-limit <0-64>
```

Parameters

```
smart-aggregation {delay [background|best-effort|streaming-video|
video-conferencing|voice] <0-1000>}
```

delay	Configures the maximum delay parameter based on the traffic type
background	Configures the maximum delay parameter, in milliseconds, for background traffic
best-effort	Configures the maximum delay parameter, in milliseconds, for best effort traffic
streaming-video	Configures the maximum delay parameter, in milliseconds, for streaming video traffic
video-conferencing	Configures the maximum delay parameter, in milliseconds, for video conferencing traffic
voice	Configures the maximum delay parameter, in milliseconds, for voice traffic
<0-1000>	This parameter is common to all of the above traffic types. • <0-1000> – Specify a value from 0 msec - 1000 msec.

```
smart-aggregation min-aggregation-limit <0-64>
```

min-aggregation-limit <0-64>	Sets the minimum number of aggregates buffered before an aggregate is sent • <0-64> – Specify a value from 0 - 64.

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

wmm

radio-qos-policy

Configures 802.11e *wireless multimedia* (wmm) parameters

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 parameters
wmm best-effort	Configures best effort access category wireless multimedia parameters
wmm video	Configures video access category wireless multimedia parameters
wmm voice	Configures voice access category wireless multimedia parameters
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 2. • 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 2. • <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 10. • voice – Sets CW Max for voice traffic. The default is 3. • video – Sets CW Max for video traffic. The default is 4 • <0-15> – ECW: the contention window. The actual value used is (2^ECW - 1). 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. • <0-15> – ECW: the contention window. The actual value used is (2^ECW - 1). 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 2. • video – Sets TXOP for video traffic. The default is 94. • <0-65535> – Specify a value from 0 - 65535 to configure the transmit opportunity limit in 32 microsecond units. 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

19

Role-Policy

In this chapter

This chapter summarizes the role policy commands in the CLI command structure.

A role policy defines the rules that associates tasks and devices with specific roles. A role is as a class of users with a specific set of requirements and responsibilities. By defining roles, you are actually defining different user groups.

A well defined role policy simplifies user management, and is a significant aspect of WLAN management.

Define wireless client roles to filter clients based on matching policies. Matching policies (much like ACLs) are sequential collections of permit and deny conditions that apply to packets received from connected clients. When a packet is received from a client, the wireless controller or access point compares the fields in the packet against applied matching policy rules to verify the packet has the required permissions to be forwarded, based on the criteria specified. If a packet does not meet any of the criteria specified it is dropped.

Additionally, wireless client connections are also managed by granting or restricting access by specifying a range of IP or MAC addresses to include or exclude from connectivity. These MAC or IP access control mechanisms are configured as firewall rules to further refine client filter and matching criteria.

Use the (config-role-policy) instance to configure role policy related configuration commands. To navigate to the
config-role instance, use the following commands:

```
rfs7000-37FABE(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-mode        Change the ldap mode
  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-test)#
```

role-policy

Table 55 summarizes role policy configuration commands.

TABLE 55 Role-Policy-Config Commands

Command	Description	Reference
default-role	When a client fails to find a matching role, the default action is assigned to that client	*page 19-806*
ldap-deadperiod	Configures the *Lightweight Directory Access Protocol* (LDAP) dead period interval	*page 19-807*
ldap-mode	Configures the LDAP server authentication mode	*page 19-808*
ldap-server	Configures the LDAP server settings	*page 19-809*
ldap-service	Enables the LDAP server attributes	*page 19-810*
ldap-timeout	Configures the LDAP query timeout	*page 19-810*
no	Negates a command or reverts settings to their default	*page 19-811*
user-role	Creates a role and associates it to the newly created role policy	*page 19-813*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
do	Runs commands from the EXEC mode	*page 4-165*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes information to the memory or terminal	*page 5-310*

default-role

role-policy

Assigns a default role to a wireless client that fails to find a matching role. Use this command to configure a wireless client not matching any role.

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 of a wireless client. This role is applied to a wireless client not matching any other configured role. • Use – Associates an IP or a MAC access list with the default role
[ip-access-list| mac-access-list] [in|out]	Associates an IP access list or a MAC access list with this default role • in – Applies the rule to incoming packets • out – Applies the rule to outgoing packets
<IP/MAC-ACCESS-LIST-NAME>	Specifies IP access list or MAC access list name • <IP/MAC-ACCESS-LIST-NAME> – Specify the IP access list name.
precedence <1-100>	After specifying the IP/MAC access list, specify the access list precedence value. • precedence – Based on the packets received, the lower precedence value is evaluated first • <1-100> – Sets a precedence value from 1 - 100

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 default role configuration
ip-access-list	Creates a new IP based access list. Access lists control access to the network using a set of rules. Each rule specifies an action taken when a packet matches a given set of rules. If the action is deny, the packet is dropped. If the action is permit, the packet is allowed.

ldap-deadperiod

role-policy

Configures *Lightweight Directory Access Protocol* (LDAP) dead period interval for this role policy

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
ldap-deadperiod <60-300>
```

Parameters

```
ldap-deadperiod <60-300>
```

ldap-deadperiod <60-300>	Configures a LDAP dead period, in seconds, with this role policy. In case of no response from an LDAP server, it is declared dead after an interval of time. • <60-300> – Specify a the interval from 30 - 600 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 dead period

ldap-mode

role-policy

Configures the LDAP server authentication mode with this role policy

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
ldap-mode [direct|controller]
```

Parameters

```
ldap-mode [direct|controller]
```

direct	Configures LDAP authentication mode as direct (Active Directory authentication)
controller	Configures LDAP authentication mode as wireless controller based. This is the default setting.

Example

```
rfs7000-37FABE(config-role-policy-test)#ldap-mode direct

rfs7000-37FABE(config-role-policy-test)#show context
role-policy test
 default-role use ip-access-list in test precedence 1
 ldap-deadperiod 100
 ldap-mode direct
```

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

Related Commands:

no	Removes or resets LDAP server authentication mode to default (controller)

ldap-server

role-policy

Asscoiates a specified LDAP server (identified by its index number) with this role policy.

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
ldap-server <1-2> host [<IP>|<HOSTNAME>] bind-dn <BIND-DN> base-dn <BASE-DN>
bind-password <PASSWORD> {port <1-65535>}
```

Parameters

```
ldap-server <1-2> host [<IP>|<HOSTNAME>] bind-dn <BIND-DN> base-dn <BASE-DN>
bind-password <PASSWORD> {port <1-65535>}
```

ldap-server <1-2>	Specify the LDAP server ID from 1 - 2.
host [<IP>|<HOST>]	Specify the LDAP server's IP address or hostname.
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).

Example

```
rfs7000-37FABE(config-role-policy-test)#ldap-server 1 host 172.16.10.10
bind-dn test base-dn test2 bind-password Testing@123 port 2

rfs7000-37FABE(config-role-policy-test)#show context
role-policy test
 default-role use ip-access-list in test precedence 1
 ldap-deadperiod 100
 ldap-mode direct
 ldap-server 1 host 172.16.10.10 bind-dn test base-dn test2 bind-password
Testing@123 port 2
rfs7000-37FABE(config-role-policy-test)#
```

Related Commands:

no	Removes or resets LDAP server index number

ldap-service

role-policy

Enables the LDAP server attributes

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
ldap-service
```

Parameters

None

Example

```
rfs7000-37FABE(config-role-policy-test)#ldap-service

rfs7000-37FABE(config-role-policy-test)#show context
role-policy test
 default-role use ip-access-list in test precedence 1
 ldap-service
 ldap-deadperiod 100
 ldap-mode direct
 ldap-server 1 host 172.16.10.10 bind-dn test base-dn test2 bind-password
Testing@123 port 2
rfs7000-37FABE(config-role-policy-test)#
```

Related Commands:

no	Removes or resets the LDAP server attributes with a user role

ldap-timeout

role-policy

Configures the LDAP query timeout interval

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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)

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-service
 ldap-timeout 1
 ldap-deadperiod 100
 ldap-mode direct
 ldap-server 1 host 172.16.10.10 bind-dn test base-dn test2 bind-password
Testing@123 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 the default role assigned to a wireless client. It also disables existing user roles from being assigned to new users.

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
no [default-role|ldap-deadperiod|ldap-mode|ldap-server <1-2>|ldap-service|
          ldap-timeout| user-role]

no [ldap-deadperiod|ldap-mode|ldap-server <1-2>|ldap-service|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-mode|ldap-server <1-2>|ldap-service|ldap-timeout]
```

no ldap-deadperiod	Resets the LDAP dead period to default
no ldap-mode	Resets the LDAP mode to default (controller)
no ldap-server <1-2>	Resets the LDAP server's index. Specify the LDAP server index.

no ldap-service	Disables the LDAP server attributes in the role definitions
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 with the default role • 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>	After specifying the IP or MAC access list, specify the ACL precedence value applied. • precedence – Based on the packets received, the lower precedence value is evaluated first. • <1-100> – Specify the precedence value from 1 - 100.

```
no user-role <ROLE-NAME>
```

no user-role <ROLE-NAME>	Deletes a user role • <ROLE-NAME> – Specify user 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-service
 ldap-timeout 1
 ldap-deadperiod 100
 ldap-mode direct
 ldap-server 1 host 172.16.10.10 bind-dn test base-dn test2 bind-password
Testing@123 port 2
rfs7000-37FABE(config-role-policy-test)#

rfs7000-37FABE(config-role-policy-test)#no ldap-service
rfs7000-37FABE(config-role-policy-test)#no ldap-deadperiod
rfs7000-37FABE(config-role-policy-test)#no ldap-timeout

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-mode direct
 ldap-server 1 host 172.16.10.10 bind-dn test base-dn test2 bind-password
Testing@123 port 2
rfs7000-37FABE(config-role-policy-test)#
```

Related Commands:

default-role	Assigns a default role to a wireless client
ldap-deadperiod	Configures the LDAP dead period interval
ldap-mode	Configures the LDAP server authentication mode
ldap-server	Configures the LDAP server settings
ldap-service	Enables the LDAP server attributes
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 and associates it to a role policy. Each user role has a set of Active Directory attributes that determine the user role. Each attribute is matched until a complete match of role policy is found.

Table 56 summarizes user role configuration commands.

TABLE 56 User-Role-Config Commands

user-role	Creates a new user role and enters its configuration mode	*page 19-813*
user-role commands	Summarizes user role configuration mode commands	*page 19-814*

user-role

user-role

Creates a user defined role

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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. Specify a name for this user role.
precedence <1-10000>	Sets the precedence for this role. If a wireless client matches multiple roles, the role with the lower precedence number (higher priority) is selected. Lower the precedence number, higher is the role priority

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:
  ap-location          AP Location configuration
  authentication-type  Type of Authentication
  captive-portal       Captive-portal based Role Filter
  city                 City configuration
  company              Company configuration
  country              Country configuration
  department           Department configuration
  emailid              Emailid configuration
  employeeid           Employeeid configuration
  encryption-type      Type of encryption
  group                Group 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
  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 a user role

user-role commands

user-role

Table 57 summarizes user role configuration mode commands.

TABLE 57 User-Role-Mode Commands

Commands	Description	Reference
ap-location	Sets an AP's deployment location	*page 19-815*
authentication-type	Selects an authentication type for a user role	*page 19-816*
captive-portal	Defines a captive portal role based filter	*page 19-817*
city	Configures a wireless client filter option based on the city name	*page 19-818*
company	Configures a wireless client filter option based on the company name	*page 19-819*

TABLE 57 User-Role-Mode Commands

Commands	Description	Reference
country	Configures a wireless client filter option based on the country name	*page 19-820*
department	Configures a wireless client filter option based on the department name	*page 19-821*
emailid	Configures a wireless client filter option based on the e-mail ID	*page 19-822*
employeeid	Configures a wireless client filter option based on the employee ID	*page 19-823*
encryption-type	Selects the encryption type	*page 19-824*
group	Sets a group configuration for the role	*page 19-825*
mu-mac	Configures the client MAC addresses for the role based firewall	*page 19-826*
no	Negates a command or sets its default	*page 19-827*
ssid	Specifies a SSID	*page 19-830*
state	Configures a user role state to match with this user role	*page 19-831*
title	Configures a 'title' string to match with this user role	*page 19-832*
use	Defines the settings used with the role policy	*page 19-832*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
do	Runs commands from the EXEC mode	*page 4-165*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes information to the memory or terminal	*page 5-310*

ap-location

user-role commands

Sets an access point's (AP's) deployment location

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
ap-location [any|contains|exact|not-contains]

ap-location any

ap-location [contains|exact|not-contains] <WORD>
```

Parameters

```
ap-location any
```

ap-location any	Specifies the location of an AP matched in a RF Domain or the AP's resident configuration. • any – Defines an AP's location as any

```
ap-location [contains|exact|not-contains] <WORD>
```

ap-location	Specifies the location of an AP matched in a RF Domain or the AP's resident configuration. Select one of the following filter options: contains, exact, not-contains
contains <WORD>	Defines an AP location that contains a specified string. The role is applied to APs whose location contains the location string specified in the role. • <WORD> – Specify the string to match
exact <WORD>	Defines an AP location that contains the exact specified string. The role is applied to APs whose location exactly matches the string specified in the role. • <WORD> – Specify the exact string to match
not-contains <WORD>	Defines an AP location that does not contain the string. The role is applied to APs whose location does not contain the location string specified in the role. • <WORD> – Specify the string not to match

Example

```
rfs7000-37FABE(config-role-policy-test-user-role-testing)#ap-location
contains office

rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
  ap-location contains office
rfs7000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands:

no	Removes an AP's deployment location from this user role

authentication-type

user-role commands

Selects the authentication type for this user role

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 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 role.
neq [eap|kerberos| mac-auth|none]	The role is applied only when the authentication type does not match 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 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
  ap-location contains office
rfs7000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands:

no	Removes the authentication type configured for this user role

captive-portal

user-role commands

Defines the captive portal based role filter for this user role

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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
post-login	Specifies authentication is completed successfully
pre-login	Specifies authentication is pending

```
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
  ap-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 option based on the city name

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 option 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-contains
any	No specific city associated with this user role. This user role can be applied to any wireless client from any city
contains <WORD>	The role is applied only when the city name 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 exact city string is 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 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
  ap-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 role

company

user-role commands

Configures a wireless client filter option based on the company name

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 option 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 role. This user role can be applied to any wireless client from any company (no strings to match)
contains <WORD>	The role is applied only when the company name 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 exact company string is 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 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
exampleutions

rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
  authentication-type eq kerberos
  ap-location contains office
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact exampleutions
rfs7000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands:

no	Removes the company name configured with this user role

country

user-role commands

Configures a wireless client filter option based on the country name

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 option 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 role. This user role can be applied to any wireless client from any country (no strings to match)
contains <WORD>	The role is applied only when the country name 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 exact country string is 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 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
  ap-location contains office
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact exampleutions
  country exact America
rfs7000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands:

no	Removes the country name configured with this user role

department

user-role commands

Configures a wireless client filter option based on the department name

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 option 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 role. This user role can be applied to any wireless client from any department (no strings to match)
contains <WORD>	The role is applied only when the department name 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 exact department string is 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 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
  ap-location contains office
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact exampleutions
  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 role

emailid

user-role commands

Configures a wireless client filter option based on the e-mail ID

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 option 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 role. This user role can be applied to any wireless client having any e-mail ID (no strings to match)
contains <WORD>	The role is applied only when the e-mail ID 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 exact e-mail ID string is 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 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@
example.com

rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
  authentication-type eq kerberos
  ap-location contains office
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact exampleutions
  country exact America
  department exact TnV
  emailid exact testing@example.com
rfs7000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands:

no	Removes the e-mail ID configured with this user role

employeeid

user-role commands

Configures a wireless client filter option based on the employee ID

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 option 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 role. This user role can be applied to any wireless client having any employee ID (no strings to match)

contains <WORD>	The role is applied only when the employee ID 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 exact employee ID string is 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 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
  ap-location contains office
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact exampleutions
  country exact America
  department exact TnV
  emailid exact testing@example.com
  employeeid contains TnVMoto
rfs7000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands:

no	Removes the employee ID configured with this user role

encryption-type

user-role commands

Selects the encryption type for this user 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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)

`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 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 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
  ap-location contains office
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact exampleutions
  country exact America
  department exact TnV
  emailid exact testing@example.com
  employeeid contains TnVMoto
rfs7000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands:

no	Removes the encryption type configured for this user role

group

user-role commands

Configures a wireless client filter option based on the RADIUS group name

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 option 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 role can fit into any group (no strings to match)
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 exact RADIUS group name string is 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
  ap-location contains office
  group contains testgroup
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact exampleutions
  country exact America
  department exact TnV
  emailid exact testing@example.com
  employeeid contains TnVMoto
rfs7000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands:

no	Removes the group configured for this user role

mu-mac

user-role commands

Configures a client's MAC addresses for the role based firewall

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
mu-mac [<MAC>|any]

mu-mac any

mu-mac <MAC> {mask <MAC>}
```

Parameters

```
mu-mac any
```

any	Matches a wireless client with any MAC address

```
mu-mac <MAC> {mask <MAC>}
```

<MAC>	Matches a specific MAC address with the allowed wireless client • <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.

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
  ap-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 exampleutions
  country exact America
  department exact TnV
  emailid exact testing@example.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 role

no

user-role commands

Negates a command or resets configured settings to their default. When used in the config role policy user 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
no [ap-location|authentication-type|captive-portal|encryption-type|group|
mu-mac|
          ssid|use]

no [ap-location|authentication-type|encryption-type|group|mu-mac|ssid]

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 [ap-location|authentication-type|encryption-type|group|mu-mac|ssid]`

no ap-location	Removes an AP's deployment location from a user role
no authentication-type	Removes the authentication type configured for a user role
no encryption-type	Removes the encryption type configured for a user role
no group	Removes the RADIUS group name configured for a user role
no mu-mac	Removes the MAC address and mask configured for a user role
no ssid	Removes the SSID configured for a user role

`no captive-portal authentication-state`

no captive-portal	Removes the captive portal based role filter configured for a user role
authentication-state	Reverts the authentication state to default

`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 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
<IPMAC-ACCESS-LIST-NAME>	Specifies the IP or MAC access list name
precedence <1-100>	Removes the access list precedence • <1-100> – Specifies 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
  ap-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 exampleutions
  country exact America
  department exact TnV
  emailid exact testing@example.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 ap-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 exampleutions
  country exact America
  department exact TnV
  emailid exact testing@example.com
rfs7000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands:

ap-location	Sets an AP’s deployment location
authentication-type	Selects the authentication type for a user role
captive-portal	Defines a captive portal based role filter for a user role
city	Configures a wireless client filter option based on the city name
company	Configures a wireless client filter option based on the company name
country	Configures a wireless client filter option based on the country name
department	Configures a wireless client filter option based on the department name
emailid	Configures a wireless client filter option based on the e-mail ID
employeeid	Configures a wireless client filter option based on the employee ID
encryption-type	Selects the encryption type used for a user role

group	Configures a group for a user role
mu-mac	Configures the client's MAC addresses for the role based firewall
ssid	Configures a user role SSID
state	Configures a user role state to match for a user role
title	Configures a user role title to match for a user role
use	Defines the access list settings used with a user role

ssid

user-role commands

Configures a user role SSID

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 option 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 option 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 exact SSID string specified in the role is matched. • <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 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.
ssid not-contains <WORD>	The role is applied only when the SSID 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 exampleutions
  country exact America
  department exact TnV
  emailid exact testing@example.com
rfs7000-37FABE(config-role-policy-test-user-role-testing)#]
```

Related Commands:

no	Removes the SSID configured for a user role

state

user-role commands

Configures a user role state to match with this user role

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 exact RADIUS state string is 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 exampleutions
  country exact America
  department exact TnV
  emailid exact testing@example.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 with this user role

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 option based on how the RADIUS title 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 RADIUS title 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 exact RADIUS title string is 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 RADIUS title 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 firewalls 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 exampleutions
  country exact America
  department exact TnV
  emailid exact testing@example.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

Chapter

Smart-RF-Policy

20

In this chapter

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 reconfiguration 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.

Use the (config) instance to configure Smart RF Policy related configuration commands. To navigate to the Smart RF policy instance, use the following commands:

```
rfs7000-37FABE(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
  root-recovery           Recover issues due to poor root path metric
  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

Table 58 summarizes Smart RF policy configuration commands.

TABLE 58 Smart-RF-Policy-Config Commands

Command	Description	Reference
area	Configures the channel list and power for a specified area	*page 20-837*
assignable-power	Specifies the power range during power assignment	*page 20-838*
channel-list	Assigns the channel list for the selected frequency	*page 20-839*
channel-width	Selects the channel width for Smart RF configuration	*page 20-839*
coverage-hole-recovery	Enables recovery from errors	*page 20-841*
enable	Enables a Smart RF policy	*page 20-842*
group-by	Configures grouping parameters	*page 20-843*

TABLE 58 Smart-RF-Policy-Config Commands

Command	Description	Reference
interference-recovery	Recovers issues due to excessive noise and interference	*page 20-843*
neighbor-recovery	Enables recovery from errors due to faulty neighbor radios	*page 20-845*
no	Negates a command or reverts settings to their default	*page 20-846*
root-recovery	Enables recovery from issues due to poor root path metric	*page 20-848*
sensitivity	Configures Smart RF sensitivity	*page 20-849*
smart-ocs-monitoring	Applies smart off channel scanning instead of dedicated detectors	*page 20-850*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
do	Runs commands from the EXEC mode	*page 4-165*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes the system running configuration to memory or terminal	*page 5-310*

area

smart-rf-policy

Configures the channel list and power for a specified area

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
channel-width [2.4GHz|5GHz] [20MHz|40MHz|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|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 or 40 MHz channel width

Usage Guidelines:

The 20/40 MHz operation (the default setting for the 5.0 GHz radio) allows the access point to receive packets from clients using
20 MHz while transmitting a packet 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

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 for a client as seen by the access point radio. If a client's signal to noise value is above the threshold, the transmit power is increased until the signal to noise rate falls below the threshold.

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 below *Signal-to-Noise Ratio* (SNR) threshold required 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 coverage hole recovery is performed after a coverage hole is detected
interval	Optional. Specifies the interval coverage hole recovery is performed 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. coverage-interval – The default is 10 seconds. 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. coverage-interval – The default is 10 seconds. interval – The default is 30 seconds.

```
coverage-hole-recovery {snr-threshold} [2.4Ghz|5Ghz] <1-75>
```

snr-threshold	Optional. Specifies the SNR threshold value. This value is the signal to noise ratio 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 the 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

Configures Smart RF grouping values

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
group-by [area|floor]
```

Parameters

```
group-by [area|floor]
```

area	Configures a group based on area
floor	Configures a group based on floor

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 when excess noise and interference is detected within the Smart RF supported radio coverage area. Smart RF provides mitigation from interference 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 can select 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
interference-recovery {channel-hold-time|channel-switch-delta|
client-threshold|
          interference|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|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 for a channel change. This parameter is the difference between noise levels on the current channel and a prospective channel. If the difference is below the configured threshold, the channel will not change.
[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|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 3,600 seconds.
client-threshold <1-255>	Optional. Specifies client thresholds to avoid channel changes (when exceeded). When the threshold number of clients are connected to a radio, it does not change its channel even though it requires one, based on the interference recovery determination made by the smart master. • <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.

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 for non WiFi interference • <1.0-3.0> – Specify the noise factor from 1.0 - 3.0

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 neighbor radios. Enabling neighbor recovery ensures automatic recovery when a radio fails 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 change • <1-10> – Sets the number of retries from 1 - 10
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

`neighbor-recovery {power-hold-time} <0-3600>`

power-hold-time	Optional. Specifies the minimum time between two power change recoveries
<0-3600>	Sets the time from 0 sec - 3600 sec. The default is 0 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
no [area|assignable-power|channel-list|channel-width|
coverage-hole-recovery|enable|
          group-by|interference-recovery|neighbor-recovery|root-recovery|
          smart-ocs-monitoring]
```

Parameters

```
no [areaassignable-power|channel-list|channel-width|
coverage-hole-recovery|enable|
group-by|interference-recovery|neighbor-recovery|
root-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 BR7161 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
root-recovery	Enables recovery from issues arising from poor root path metric
smart-ocs-monitoring	Applies smart off channel scanning instead of dedicated detectors

root-recovery

smart-rf-policy

Enables recovery from issues arising due a poor root path metric

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
root-recovery {root-path-metric-threshold|root-recovery-time}
root-recovery {root-path-metric-threshold <1-65535>|root-recovery-time
<1-20>}
```

Parameters

```
root-recovery {root-path-metric-threshold <1-65535>|root-recovery-time
<1-20>}
```

root-path-metric-threshold <1-65535>	Optional. Configures the minimum root path metric threshold When this threshold is exceeded, a channel switch may occur. • <1-65535> – Specify a value from 1 - 65536.
root-recovery-time <1-20>	Optional. Configures the recovery time, in minutes, from loss of path to the root • <1-20> – Specify a value from 1 - 20 minutes.

Example

```
rfs7000-37FABE(config-smart-rf-policy-test)#root-recovery root-recovery-time
15
rfs7000-37FABE(config-smart-rf-policy-test)#root-recovery
root-path-metric-threshold 100

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
 root-recovery root-path-metric-threshold 100
 root-recovery root-recovery-time 15
 coverage-hole-recovery snr-threshold 5GHz 1
rfs7000-37FABE(config-smart-rf-policy-test)#
```

Related Commands:

no	Disabled recovery from issues arising due a poor root path metric

sensitivity

smart-rf-policy

Configures Smart RF sensitivity

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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:

The Power Settings and Channel Settings parameters are enabled only when Sensitivity is set to Custom or Medium.

The monitoring and scanning parameters are enabled only when Sensitivity is set to Custom.

The Neighbor Recovery, Interference and Coverage Hole Recovery parameters are enabled only when Sensitivity is set 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
 smart-ocs-monitoring extended-scan-frequency 5GHz 0
 smart-ocs-monitoring extended-scan-frequency 2.4GHz 0
 --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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
smart-ocs-monitoring {client-aware|extended-scan-frequency|frequency|

meshpoint|off-channel-duration|power-save-aware|sample-count|voice-aware}
```

```
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 {meshpoint} [2.4GHz|5GHz] <MESHPOINT-NAME>

smart-ocs-monitoring {off-channel-duration} [2.4GHz|5GHz] <20-150>

smart-ocs-monitoring {power-save-aware} [2.4GHz|5GHz] [dynamic|strict]

smart-ocs-monitoring {sample-count} [2.4GHz|5GHz] <1-15>

smart-ocs-monitoring {voice-aware} [2.4GHz|5GHz] [dynamic|strict]
```

Parameters

`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 does not change its channel even if needed (based on the interference recovery determination made by the smart master)
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 50 clients.
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 50 clients.

`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 frequency the channel must be switched. Sets the value, in seconds, from 1 - 120
2.4GHz <1-120>	Selects the 2.4 GHz band • <1-120> – Sets a scan frequency from 1 sec - 120 sec. The default is 6 seconds.
5GHz <1-120>	Selects the 5.0 GHz band • <1-120> – Sets a scan frequency from 1 sec - 120 sec. The default is 6 seconds.

`smart-ocs-monitoring {meshpoint} [2.4GHz|5GHz] <MESHPOINT-NAME>`

meshpoint	Optional. Specifies the meshpoint to monitor

2.4GHz <MESHPOINT-NAME>	Enables meshpoint monitoring on 2.4 GHz band • <MESHPOINT-NAME> – Specify the meshpoint name.
5GHz <MESHPOINT-NAME>	Enables meshpoint monitoring on 5.0 GHz band • <MESHPOINT-NAME> – Specify the meshpoint name.

`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 msec - 150 msec. The default is 50 msec.
5GHz <20-150>	Selects the 5.0 GHz band (in milliseconds) • <20-150> – Sets the off channel duration from 20 msec - 150 msec. The default is 50 milliseconds.

`smart-ocs-monitoring {power-save-aware} [2.4GHz|5GHz] [dynamic|strict]`

power-save-aware	Optional. Enables power save aware scanning on this Smart RF policy
2.4GHz [dynamic|strict]	Sets power save aware scanning mode on the 2.4 GHz band • dynamic – Dynamically avoids scanning based on traffic for *power save* (PSP) clients • strict – Strictly avoids scanning when PSP clients are present
5GHz [dynamic|strict]	Sets power save aware scanning mode on the 5.0 GHz band • dynamic – Dynamically avoids scanning based on traffic for PSP clients • strict – Strictly avoids scanning when PSP clients are present

`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 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 5.
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] [dynamic|strict]`

voice-aware	Optional. Enables voice aware scanning on this Smart RF policy
2.4GHz [dynamic|strict]	Specifies the scanning mode on the 2.4 GHz band • dynamic – Dynamically avoids scanning based on traffic for voice clients • strict – Strictly avoids scanning when voice clients are present 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. 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

20

Chapter

WIPS-Policy

21

In this chapter

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.

Brocade Mobility supports WIPS through the use of sensor devices that locate unauthorized access points.

Unauthorized APs are untrusted access points connected to a LAN accepting 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 an 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 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 wireless controller managed wireless network.
- *Rogue Detection and Segregation* - WIPS distinguishes itself by both 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 APs). The correct classification of potential threats is critical 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 network. This allows for the removal of potential rogues though 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 enables organizations to operate WEP encrypted networks securely and to preserve their existing investment in mobile devices.

Use the (config) instance to configure WIPS policy commands. To navigate to the WIPS policy instance, use the following commands:

```
rfs7000-37FABE(config)#wips-policy <POLICY-NAME>
rfs7000-37FABE(config)#wips-policy test
rfs7000-37FABE(config-wips-policy-test)#?
Wips Policy Mode commands:
  ap-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

Table 59 summarizes WIPS policy configuration commands.

TABLE 59 WIPS-Policy-Config Commands

Command	Description	Reference
ap-detection	Defines the WIPS AP detection configuration	*page 21-857*
enable	Enables a WIPS policy	*page 21-858*
event	Configures events	*page 21-858*
history-throttle-duration	Configures the duration event duplicates are omitted from the event history	*page 21-861*
interference-event	Specifies events contributing to the Smart RF WiFi interference calculations	*page 21-862*
no	Negates a command or sets its default	*page 21-863*
signature	Configures a WIPS policy signature and enters its configuration mode	*page 21-867*
use	Defines a WIPS policy settings	*page 21-879*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
do	Runs commands from the EXEC mode	*page 4-165*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*

TABLE 59 WIPS-Policy-Config Commands

Command	Description	Reference
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug **(config-if)** instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes the system running configuration to memory or terminal	*page 5-310*

ap-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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
ap-detection {ageout|wait-time}
ap-detection {age-out <30-86400>|wait-time <10-600>}
```

Parameters

```
ap-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)#ap-detection wait-time 15
rfs7000-37FABE(config-wips-policy-test)#ap-detection age-out 50

rfs7000-37FABE(config-wips-policy-test)#show context
wips-policy test
 ap-detection-ageout 50
 ap-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

Associates this WIPS policy with a profile

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 from use with a profile

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
event [ap-anomaly|client-anomaly|enable-all-events|excessive]
```

```
event ap-anomaly [ad-hoc-violation|airjack|ap-ssid-broadcast-in-beacon|
asleap|
          impersonation-attack|null-probe-response|
transmitting-device-using-invalid-mac|
          unencrypted-wired-leakage|wireless-bridge]

event client-anomaly [crackable-wep-iv-key-used|dos-broadcast-deauth|
          fuzzing-all-zero-macs|fuzzing-invalid-frame-type|
fuzzing-invalid-mgmt-frames|
          fuzzing-invalid-seq-num|
identical-src-and-dest-addr|invalid-8021x-frames|
          netstumbler-generic|non-changing-wep-iv|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-station]
          {filter-ageout <0-86400>|threshold-client <0-65535>|threshold-radio
<0-65535>}
```

Parameters

```
event ap-anomaly
[ad-hoc-violation|airjack|ap-ssid-broadcast-in-beacon|asleap|
impersonation-attack|null-probe-response|transmitting-device-using-invalid-ma
c|
unencrypted-wired-leakage|wireless-bridge]
```

ap-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
ap-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 [crackable-wep-iv-key-used|dos-broadcast-deauth|
fuzzing-all-zero-macs|fuzzing-invalid-frame-type|fuzzing-invalid-mgmt-frames|
fuzzing-invalid-seq-num|identical-src-and-dest-addr|invalid-8021x-frames|
netstumbler-generic|non-changing-wep-iv|non-conforming-data|tkip-mic-counter-
measures|
wellenreiter] {filter-ageout <0-86400>}
```

client-anomaly	Enables client anomaly event tracking These are suspicious events performed by wireless clients that compromising the security of the network. An administrator can enable or disable the filtering of each listed event and set the thresholds required for the generation of the event notification and filtering action applied.
crackable-wep-iv-key-used	Tracks the use of a crackable WEP IV Key
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-changing-wep-iv	Tracks unchanging WEP IV events
non-conforming-data	Tracks non conforming data packets
tkip-mic-counter-measures	Tracks TKIP MIC counter measures caused by station
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. 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.

```
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. 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. 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
 ap-detection-ageout 50
 ap-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

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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
 ap-detection-ageout 50
 ap-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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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
 ap-detection-ageout 50
 ap-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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
no [ap-detection|enable|event|history-throttle-duration|interference-event|
           signature|use]

no [enable|history-throttle-duration]

no ap-detection {ageout|wait-time} {<LINE-SINK>}

no event [ap-anomaly|client-anomaly|enable-all-events|excessive]

no event ap-anomaly [ad-hoc-violation|airjack|ap-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 [crackable-wep-iv-key-used|dos-broadcast-deauth|
          fuzzing-all-zero-macs|fuzzing-invalid-frame-type|
fuzzing-invalid-mgmt-frames|
          fuzzing-invalid-seq-num|
identical-src-and-dest-addr|invalid-8021x-frames|
          netstumbler-generic|non-changing-wep-iv|non-conforming-data|
          tkip-mic-counter-measures|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 ap-detection {ageout|wait-time} {<LINE-SINK>}
```

no ap-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 ap-anomaly [ad-hoc-violation|airjack|ap-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
ap-anomaly	Disables AP anomaly event tracking
ad-hoc-violation	Disables ad-hoc network violation event tracking
airjack	Disables the tracking of AirJack attacks
ap-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 [crackable-wep-iv-key-used|dos-broadcast-deauth|
      fuzzing-all-zero-macs|fuzzing-invalid-frame-type|
fuzzing-invalid-mgmt-frames|
fuzzing-invalid-seq-num|identical-src-and-dest-addr|invalid-8021x-frames|
netstumbler-generic|non-changing-wep-iv|non-conforming-data|
tkip-mic-counter-measures|wellenreiter] {filter-ageout <0-86400>}
```

no event	Disables WIPS policy event tracking
client-anomaly	Disables client anomaly event tracking
crackable-wep-iv-key-used	Disables the tracking of a crackable WEP IV Key usage
dos-broadcast-deauth	Disables DoS broadcast deauthentication event tracking
fuzzing-all-zero-macs	Disables the tracking of Fuzzing: All zero MAC addresses observed
fuzzing-invalid-frame-type	Disables the tracking of Fuzzing: Invalid frame type detected
fuzzing-invalid-mgmt-frames	Disables the tracking of Fuzzing: Invalid management frame
fuzzing-invalid-seq-num	Disables the tracking of Fuzzing: Invalid sequence number
identical-src-and-dest-addr	Disables the tracking of identical source and destination addresses
invalid-8021x-frames	Disables the tracking of Fuzzing: Invalid 802.1x frames
netstumbler-generic	Disables Netstumbler (v3.2.0, 3.2.3, 3.3.0) event tracking
non-changing-wep-iv	Disables unchanging WEP IV event tracking
non-conforming-data	Disables non conforming data packet tracking
tkip-mic-counter-measures	Disables the tracking of TKIP MIC counter measures caused by a client
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
 ap-detection-ageout 50
 ap-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
 ap-detection-ageout 50
 ap-detection-wait-time 15
rfs7000-37FABE(config-wips-policy-test)#
```

Related Commands:

ap-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.

Table 60 summarizes WIPS policy signature configuration commands.

TABLE 60 WIPS-Policy-Signature-Config Commands

signature	Configures a WIPS policy signature and enters its configuration mode	*page 21-867*
signature mode commands	Summarizes WIPS signature configuration mode commands	*page 21-868*

signature

signature

Configures a WIPS policy signature

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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)#show context
signature test
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
 ap-detection-ageout 50
 ap-detection-wait-time 15
rfs7000-37FABE(config-wips-policy-test)#
```

Related Commands:

no	Deletes a WIPS policy signature

signature mode commands

signature

Table 61 summarizes WIPS policy signature configuration mode commands.

TABLE 61 WIPS-Policy-Signature-Mode Commands

Commands	Description	Reference
bssid	Configures the BSSID MAC address	*page 21-869*
dst-mac	Configures the destination MAC address	*page 21-870*
filter-ageout	Configures the filter ageout interval	*page 21-870*
frame-type	Configures the frame type used for matching	*page 21-871*
interference-event	Configures this WIPS policy signature as the Smart RF interference source	*page 21-872*
mode	Enables or disables the signature mode	*page 21-873*
payload	Configures payload settings	*page 21-873*
src-mac	Configures the source MAC address	*page 21-874*
ssid-match	Configures a match based on SSID	*page 21-875*

TABLE 61 WIPS-Policy-Signature-Mode Commands

Commands	Description	Reference
threshold-client	Configures the wireless client threshold limit	*page 21-876*
threshold-radio	Configures the radio threshold limit	*page 21-876*
no	Negates a command or sets its default	*page 21-877*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
do	Runs commands from the EXEC mode	*page 4-165*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug (config-if) instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes the system running configuration to memory or terminal	*page 5-310*

bssid

signature mode commands

Configures a BSSID MAC address with this WIPS signature for matching

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
bssid <MAC>
```

Parameters

```
bssid <MAC>
```

bssid <MAC>	Configures a BSSID MAC address with this signature • <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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
dst-mac <MAC>
```

Parameters

```
dst-mac <MAC>
```

dst-mac <MAC>	Configures a destination MAC address with this WIPS signature • <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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
interference
```

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 mode

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
mode enable
```

Parameters

```
mode enable
```

mode enable	Enables signature mode

Example

```
rfs7000-37FABE(config-test-signature-test)#mode enable
rfs7000-37FABE(config-test-signature-test)#
```

Related Commands:

no	Disables a WIPS signature mode

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 index 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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. Specify the correct SSID to ensure proper filtering.
ssid-len <0-32>	Specifies the character 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 300 Access Point, , Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
no
[bssid|dst-mac|filter-ageout|frame-type|interferenc-event|mode|payload|src-ma
c|
          ssid-match|   threshold-client|threshold-radio]

no [bssid|dts-mac|filter-ageout|frame-type|interference-event|mode enbale|
          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 enbale|
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)#
rfs7000-37FABE(config-test-signature-test)#no bssid
rfs7000-37FABE(config-test-signature-test)#
rfs7000-37FABE(config-test-signature-test)#no dst-mac
```

```
rfs7000-37FABE(config-test-signature-test)#
rfs7000-37FABE(config-test-signature-test)#no src-mac
rfs7000-37FABE(config-test-signature-test)#
rfs7000-37FABE(config-test-signature-test)#no filter-ageout
rfs7000-37FABE(config-test-signature-test)#
rfs7000-37FABE(config-test-signature-test)#no threshold-client
rfs7000-37FABE(config-test-signature-test)#
rfs7000-37FABE(config-test-signature-test)#no threshold-radio
rfs7000-37FABE(config-test-signature-test)#

rfs7000-37FABE(config-test-signature-test)#show context
 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, or creates a new device categorization list. The list categorizes devices as authorized or unauthorized.

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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
 ap-detection-ageout 50
 ap-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

In this chapter

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:

```
rfs7000-37FABE(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)#
```

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 62 summarizes WLAN QoS policy configuration commands.

TABLE 62 WLAN-QoS-Policy-Config Commands

Command	Description	Reference
accelerated-multicast	Configures accelerated multicast stream addresses and forwards QoS classifications	*page 22-882*
classification	Classifies WLAN traffic based on priority	*page 22-883*
multicast-mask	Configures the egress prioritization multicast mask	*page 22-885*
no	Negates a command or sets its default	*page 22-886*
qos	Defines the QoS configuration	*page 22-888*
rate-limit	Configures the WLAN traffic rate limit using a WLAN QoS policy	*page 22-889*
svp-prioritization	Enables Spectralink voice protocol support on a WLAN	*page 22-892*
voice-prioritization	Prioritizes voice client over other clients	*page 22-892*
wmm	Configures 802.11e/wireless multimedia parameters	*page 22-893*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
do	Runs commands the from EXEC mode	*page 4-165*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes the system running configuration to memory or terminal	*page 5-310*

accelerated-multicast

wlan-qos-policy

Configures the accelerated multicast stream address and forwarding QoS classification

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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. This parameter allows the system to convert multicast streams to unicast, or to specify multicast streams converted to unicast.
classification	Optional. Configures the forwarding of the QoS classification (traffic class). 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 autodetect.
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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 300 Access Point, , Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 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 300 Access Point, , Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 on 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 wireless controller are applied. An administrator can set separate QoS rate limit configurations for data transmitted from the managed network (upstream) and data transmitted from a WLAN's wireless clients back to their associated access point radios and wireless controller (downstream).

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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. 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 of any access category, 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 parameters for this WLAN QoS policy

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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)#
```

22

Chapter

Interface-Radio Commands

23

In this chapter

This chapter summarizes the interface radio commands in the CLI command structure.

Use the (config-profile-default-Brocade Mobility RFS4000) instance to configure radio instances associated with a RFS4011 model controller.

To switch to this mode, use:

```
rfs4000-37FAB(config-profile-default-rfs4000)#interface radio ?
  1  Radio interface 1
  2  Radio interface 2
  3  Radio interface 3
rfs4000-37FABE(config-profile-default-rfs4000)#interface radio
rfs4000-880DA7(config-profile-default-rfs4000-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
  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-share-mode         Configure the radio-share mode of operation for
                           this radio
  rate-selection           Default or Opportunistic rate relection
  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
  txbf                     Configure Transmit Beamforming (TxBF) parameters
                           (DEMO FEATURE)
  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

rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#
```

interface-radio instance

Interface-Radio Commands

Table 63 summarizes interface radio configuration commands.

TABLE 63 Interface-Radio-Config Commands

Commands	Description	Reference
aeroscout	Enables Aeroscout Multicast packet forwarding	*page 23-900*
aggregation	Configures 802.11n aggregation parameters	*page 23-900*
airtime-fairness	Enables fair access for clients based on airtime usage	*page 23-902*
antenna-gain	Specifies the antenna gain of the selected radio	*page 23-904*
antenna-diversity	Transmits antenna diversity for non-11n transmit rates	*page 23-903*
antenna-downtilt	Enables the *Advanced Element Panel Technology* (ADEPT) antenna mode	*page 23-904*
antenna-mode	Configures the radio antenna mode	*page 23-905*
beacon	Configures beacon parameters	*page 23-906*
channel	Configures a radio's channel of operation	*page 23-907*

TABLE 63 Interface-Radio-Config Commands

Commands	Description	Reference
data-rates	Specifies the 802.11 rates supported on a radio	*page 23-908*
dfs-rehome	Reverts to the configured home channel once the *Dynamic Frequency Selection* (DFS) evacuation period expires	*page 23-910*
description	Defines a radio's description	*page 23-910*
dynamic-chain-selection	Enables automatic antenna mode selection	*page 23-911*
ekahau	Enables Ekahau multicast packet forwarding	*page 23-911*
extended-range	Configures a radio's extended range settings	*page 23-913*
guard-interval	Configures the 802.11n guard interval	*page 23-914*
lock-rf-mode	Retains user configured radio RF mode settings	*page 23-915*
max-clients	Defines the maximum number of wireless clients allowed to associate	*page 23-916*
mesh	Configures radio mesh parameters	*page 23-917*
meshpoint	Maps an existing meshpoint to this radio	*page 23-918*
no	Negates a command or sets its default	*page 23-918*
non-unicast	Configures the handling of non unicast frames	*page 23-922*
off-channel-scan	Enables radio off channel scanning	*page 23-924*
placement	Configures the location where a radio is deployed	*page 23-925*
power	Configures the radio transmit power	*page 23-926*
preamble-short	Configures user short preambles on the radio	*page 23-927*
probe-response	Configures transmission parameters for probe response frames	*page 23-928*
radio-share-mode	Configures the radio tap mode for a radio	*page 23-929*
rate-selection	Sets the rate selection method to standard or opportunistic	*page 23-930*
rf-mode	Configures a radio RF mode	*page 23-931*
rifs	Configures *Reduced Interframe Spacing* (RIFS) parameters	*page 23-932*
rts-threshold	Configures a radio's RTS threshold value	*page 23-933*
shutdown	Terminates a selected radio interface	*page 23-934*
sniffer-redirect	Captures and redirects packets to an IP address running a packet capture/analysis tool	*page 23-934*
stbc	Configures the radio's *Space Time Block Coding* (STBC) mode.	*page 23-935*
use	Applies other configuration profiles or values on the current configuration item	*page 23-936*
wireless-client	Configures wireless client related parameters	*page 23-937*
wlan	Enables a radio WLAN	*page 23-938*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
do	Runs commands from the EXEC mode	*page 4-165*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*

TABLE 63 Interface-Radio-Config Commands

Commands	Description	Reference
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug (`config-if`) instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes the system running configuration to memory or terminal	*page 5-310*

aeroscout

interface-radio instance

Enables Aeroscout Multicast packet forwarding

Supported in the following platforms:

- Wireless Controller — RFS4011

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 multicast MAC address in the AA-BB-CC-DD-EE-FF format.

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#aeroscout mac
11-22-33-44-55-66

rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
 interface radio1
  aeroscout mac 11-22-33-44-55-66
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#
```

Related Commands:

no	Resets default Aeroscout multicast MAC address

aggregation

interface-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:

- Wireless Controller — RFS4011

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 [<0-65535>]

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
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

`aggregation ampdu max-aggr-size tx <0-65535>`

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 <0-65535>	Configures the limit on transmitted frames • <0-65535> – Sets the limit from 0 - 65536 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 • 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
tx-rx	Supports the transmission and receipt of AMSDU aggregated frames

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#aggregation ampdu
tx-only

rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
 interface radio1
  aggregation ampdu tx-only
  aeroscout mac 11-22-33-44-55-66
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#
```

Related Commands:

no	Disables 802.11n aggregation parameters

airtime-fairness

interface-radio instance

Enables equal access for wireless clients based on their airtime usage

Supported in the following platforms:

- Wireless Controller — RFS4011

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>	Configures the relative weightage for 11n clients over legacy clients. • <1-10> – Sets a weightage ratio for 11n clients from 1 - 10

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#airtime-fairness
prefer-ht weight 6

rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
 interface radio1
  aggregation ampdu tx-only
  aeroscout mac 11-22-33-44-55-66
  airtime-fairness prefer-ht weight 6
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#
```

Related Commands:

no	Disables fair access to medium for wireless clients (provides access on a round-robin mode)

antenna-diversity

interface-radio instance

Transmits antenna diversity for non-11n transmit rates

Supported in the following platforms:

- Wireless Controller — RFS4011

Syntax:

```
antenna-diversity
```

Parameters

None

Example

```
rfs4000-880DA7(config-profile-default-Brocade Mobility
RFS4000-if-radio1)#antenna-diversity

rfs4000-880DA7(config-profile-default-Brocade Mobility
RFS4000-if-radio1)#show context
```

```
 interface radio1
  aggregation ampdu tx-only
  aeroscout mac 11-22-33-44-55-66
  antenna-diversity
  airtime-fairness prefer-ht weight 6
rfs4000-880DA7(config-profile-default-Brocade Mobility RFS4000-if-radio1)#
```

Related Commands:

no	Uses single antenna for non-11n transmit rates

antenna-downtilt

interface-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

Supported in the following platforms:

- Access Point — Brocade Mobility 71XX Access Point

NOTE
This feature is not supported on a RFS4011 model controller.

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-radio instance

Configures the antenna gain value of the selected radio. Antenna gain defines the ability of an antenna to convert power into radio waves and vice versa.

Supported in the following platforms:

- Wireless Controller — RFS4011

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

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#antenna-gain 12.0

rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
 interface radio1
  antenna-gain 12.0
  aggregation ampdu tx-only
  aeroscout mac 11-22-33-44-55-66
  antenna-diversity
  airtime-fairness prefer-ht weight 6
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#
```

Related Commands:

no	Resets the antenna gain of a radio

antenna-mode

interface-radio instance

Configures the antenna mode (the number of transmit and receive antennas) on the radio

Supported in the following platforms:

- Wireless Controller — RFS4011

Syntax:

```
antenna-mode [1*1|1*3|2*2|default]
```

Parameters

```
antenna-mode [1*1|1*3|2*2|default]
```

1*1	Uses antenna A to receive and transmit
1*3	Uses antenna A to transmit and receives on other antennas
2*2	Uses antenna A and C for both transmit and receive
default	Uses default antenna settings

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#antenna-mode 1xALL

rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)# show context
```

```
 interface radio1
  antenna-gain 12.0
  aggregation ampdu tx-only
  aeroscout mac 11-22-33-44-55-66
  antenna-mode 1xALL
  antenna-diversity
  airtime-fairness prefer-ht weight 6
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#
```

Related Commands:

no	Resets the radio antenna mode (the number of transmit and receive antennas) to its default

beacon

interface-radio instance

Configures radio beacon parameters. Beacons are packets sent by the access point to synchronize a wireless network.

Supported in the following platforms:

- Wireless Controller — RFS4011

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 <1-16> <1-50>]
```

beacon	Configures radio beacon parameters
dtim-period	Configures the radio *Delivery Traffic Indication Message* (DTIM) interval. 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 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 • 50 – Configures 50 K-uSec interval between beacons • 100 – Configures 100 K-uSec interval between beacons (default) • 200 – Confgiures 200 K-uSec interval between beacons

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#beacon dtim-period
bss 2 20
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#beacon period 50
```

```
rfs4000-880DA7(config-profile-default-rfs4000-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
  beacon dtim-period bss 4 2
  beacon dtim-period bss 5 2
  beacon dtim-period bss 6 2
  beacon dtim-period bss 7 2
  beacon dtim-period bss 8 2
  --More--
```

Related Commands:

no	Resets beacon parameters to default

channel

interface-radio instance

Configures a radio's channel of operation

Supported in the following platforms:

- Wireless Controller — RFS4011

Syntax:

```
channel [smart|acs|1|2|3|4|-------]
```

Parameters

```
channel [smart|acs|1|2|3|4|-------]
```

smart|1|2|3|4|-------]	Uses Smart RF to assign a channel (uses uniform spectrum spreading if Smart RF is not enabled) • 1 – Channel 1 in 20 MHz • 2 – Channel 1 in 20 MHz

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#channel 1

rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
 interface radio1
  channel 1
  beacon period 50
  beacon dtim-period bss 1 2
  beacon dtim-period bss 2 20
  beacon dtim-period bss 3 2
  beacon dtim-period bss 4 2
  beacon dtim-period bss 5 2
  beacon dtim-period bss 6 2
  beacon dtim-period bss 7 2
  beacon dtim-period bss 8 2
  beacon dtim-period bss 9 2
  beacon dtim-period bss 10 2
  beacon dtim-period bss 11 2
  beacon dtim-period bss 12 2
  beacon dtim-period bss 13 2
```

```
  beacon dtim-period bss 14 2
  beacon dtim-period bss 15 2
  beacon dtim-period bss 16 2
  antenna-gain 12.0
  aggregation ampdu tx-only
  aeroscout mac 11-22-33-44-55-66
  antenna-mode 1xALL
--More--
```

Related Commands:

no	Resets a radio's channel of operation

data-rates

interface-radio instance

Configures the 802.11 data rates on this radio

Supported in the following platforms:

- Wireless Controller — RFS4011

Syntax:

```
data-rates [b-only|g-only|a-only|bg|bgn|gn|an|default|custom]

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|mcs0-7|mcs8-15|
mcs0-15|basic-1|
          basic-2| basic-5.5|basic-6|basic-9|basic-11|basic-12|
basic-18|basic-24|basic-36|
          basic-48|basic-54|basic-mcs0-7]]
```

Parameters

```
data-rates [b-only|g-only|a-only|bg|bgn|gn|an|default]
```

b-only	Supports operation in 11b only
g-only	Uses rates that support operation in 11g only
a-only	Uses rates that support operation in 11a only
bg	Uses rates that support both 11b and 11g wireless clients
bgn	Uses rates that support 11b, 11g and 11n wireless clients
gn	Uses rates that support 11g and 11n wireless clients
an	Uses rates that support 11a and 11n wireless clients
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|mcs0-7|mcs8-15|
mcs0-15|basic-1|basic-2| basic-5.5|basic-6|basic-9|basic-11|basic-12|
basic-18|basic-24|basic-36|basic-48|basic-54|basic-mcs0-7]
```

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 • mcs0-7 – Modulation and Coding Scheme 0-7 • mcs8-15 – Modulation and Coding Scheme 8-15 • mcs0-15 – Modulation and Coding Scheme 0-15 • 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-mcs0-7 – Modulation and Coding Scheme 0-7 as a basic rate

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#data-rates b-only

rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
 interface radio1
  channel 1
  data-rates b-only
  beacon period 50
  beacon dtim-period bss 1 2
  beacon dtim-period bss 2 20
  beacon dtim-period bss 3 2
  beacon dtim-period bss 4 2
  beacon dtim-period bss 5 2
--More--

rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#data-rates custom
basic-mcs0-7

rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
 interface radio1
  channel 1
  data-rates custom basic-mcs0-7
```

```
  beacon period 50
  beacon dtim-period bss 1 2
  beacon dtim-period bss 2 20
  beacon dtim-period bss 3 2
  beacon dtim-period bss 4 2
  beacon dtim-period bss 5 2
  beacon dtim-period bss 6 2
--More--
```

Related Commands:

no	Resets the 802.11 data rates on a radio

description

interface-radio instance

Defines a description for the selected radio

Supported in the following platforms:

- Wireless Controller — RFS4011

Syntax:

```
description <WORD>
```

Parameters

```
description <WORD>
```

<WORD>	Defines a description for the selected radio

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#description “primary
radio to use”

rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
 interface radio1
  description primary\ radio\ to\ use
  channel 1
  data-rates custom basic-mcs0-7
  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 a radio’s description

dfs-rehome

interface-radio instance

Reverts to the configured home channel once the *Dynamic Frequency Selection* (DFS) evacuation period expires

Supported in the following platforms:

- Wireless Controller — RFS4011

Syntax:

```
dfs-rehome
```

Parameters

None

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#dfs-rehome
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#
```

Related Commands:

no	Stays on the DFS elected channel after evacuation period expires

dynamic-chain-selection

interface-radio instance

Enables automatic antenna mode selection (single antenna for non-11n transmit rates)

Supported in the following platforms:

- Wireless Controller — RFS4011

Syntax:

```
dynamic-chain-selection
```

Parameters

None

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#dynamic-chain-select
ion
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#
```

Related Commands:

no	Resets automatic antenna mode selection to default

ekahau

interface-radio instance

Enables Ekahau multicast packet forwarding

Supported in the following platforms:

- Wireless Controller — RFS4011

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 *Tasman Sniffer Protocol* (TZSP) port on Ekahau engine from 0 - 65535
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

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#ekahau forward ip
172.16.10.1 port 3

rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
 interface radio1
  description primary\ radio\ to\ use
  channel 1
  data-rates custom basic-mcs0-7
  beacon period 50
  beacon dtim-period bss 1 2
  beacon dtim-period bss 2 20
  beacon dtim-period bss 3 2
  beacon dtim-period bss 4 2
  beacon dtim-period bss 5 2
  beacon dtim-period bss 6 2
  beacon dtim-period bss 7 2
  beacon dtim-period bss 8 2
  beacon dtim-period bss 9 2
  beacon dtim-period bss 10 2
  beacon dtim-period bss 11 2
  beacon dtim-period bss 12 2
  beacon dtim-period bss 13 2
  beacon dtim-period bss 14 2
  beacon dtim-period bss 15 2
  beacon dtim-period bss 16 2
  antenna-gain 12.0
  aggregation ampdu tx-only
  aeroscout mac 11-22-33-44-55-66
  ekahau forward ip 172.16.10.1 port 3
  antenna-mode 1xALL
  antenna-diversity
  airtime-fairness prefer-ht weight 6
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#
```

Related Commands:

no	Uses default Ekahau multicast MAC address

extended-range

interface-radio instance

Configures a radio's extended range settings (in kilometers)

Supported in the following platforms:

- Access Point — Brocade Mobility 71XX Access Point

NOTE
This feature is not supported on a RFS4011 model controller.

Syntax:

```
extended-range <1-25>
```

Parameters

```
extended-range <1-25>
```

extended-range <1-25>	Configures a radio's extended range settings 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--
```

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-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.

Supported in the following platforms:

- Wireless Controller — RFS4011

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)

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#guard-interval long

rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
 interface radio1
  description primary\ radio\ to\ use
  channel 1
  data-rates custom basic-mcs0-7
  beacon period 50
  beacon dtim-period bss 1 2
  beacon dtim-period bss 2 20
  beacon dtim-period bss 3 2
  beacon dtim-period bss 4 2
  beacon dtim-period bss 5 2
  beacon dtim-period bss 6 2
  beacon dtim-period bss 7 2
  beacon dtim-period bss 8 2
  beacon dtim-period bss 9 2
  beacon dtim-period bss 10 2
  beacon dtim-period bss 11 2
  beacon dtim-period bss 12 2
  beacon dtim-period bss 13 2
  beacon dtim-period bss 14 2
  beacon dtim-period bss 15 2
  beacon dtim-period bss 16 2
  antenna-gain 12.0
  guard-interval long
--More--
```

Related Commands:

no	Resets the 802.11n guard interval to default

lock-rf-mode

interface-radio instance

Retains user configured RF mode settings for the selected radio

Supported in the following platforms:

- Wireless Controller — RFS4011

Syntax:

```
lock-rf-mode
```

Parameters

None

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#lock-rf-mode

rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
 interface radio1
  description primary\ radio\ to\ use
  channel 1
  data-rates custom basic-mcs0-7
  beacon period 50
  beacon dtim-period bss 1 2
  beacon dtim-period bss 2 20
  beacon dtim-period bss 3 2
  beacon dtim-period bss 4 2
  beacon dtim-period bss 5 2
  beacon dtim-period bss 6 2
  beacon dtim-period bss 7 2
  beacon dtim-period bss 8 2
  beacon dtim-period bss 9 2
  beacon dtim-period bss 10 2
  beacon dtim-period bss 11 2
  beacon dtim-period bss 12 2
  beacon dtim-period bss 13 2
  beacon dtim-period bss 14 2
  beacon dtim-period bss 15 2
  beacon dtim-period bss 16 2
  antenna-gain 12.0
  guard-interval long
  aggregation ampdu tx-only
  aeroscout mac 11-22-33-44-55-66
  ekahau forward ip 172.16.10.1 port 3
  antenna-mode 1xALL
  antenna-diversity
  airtime-fairness prefer-ht weight 6
  lock-rf-mode
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#
```

Related Commands:

no	Allows Smart RF to change a radio's RF mode settings

max-clients

interface-radio instance

Configures the maximum number of wireless clients allowed to associate with this radio

Supported in the following platforms:

- Wireless Controller — RFS4011

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.

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#max-clients 100

rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
 interface radio1
  description primary\ radio\ to\ use
  channel 1
  data-rates custom basic-mcs0-7
  beacon period 50
  beacon dtim-period bss 1 2
  beacon dtim-period bss 2 20
  beacon dtim-period bss 3 2
  beacon dtim-period bss 4 2
  beacon dtim-period bss 5 2
  beacon dtim-period bss 6 2
  beacon dtim-period bss 7 2
  beacon dtim-period bss 8 2
  beacon dtim-period bss 9 2
  beacon dtim-period bss 10 2
  beacon dtim-period bss 11 2
  beacon dtim-period bss 12 2
  beacon dtim-period bss 13 2
  beacon dtim-period bss 14 2
  beacon dtim-period bss 15 2
  beacon dtim-period bss 16 2
  antenna-gain 12.0
  guard-interval long
  aggregation ampdu tx-only
  aeroscout mac 11-22-33-44-55-66
  ekahau forward ip 172.16.10.1 port 3
  antenna-mode 1xALL
  antenna-diversity
  max-clients 100
  airtime-fairness prefer-ht weight 6
```

```
--More--
```

Related Commands:

no	Resets the maximum number of wireless clients allowed to associate with a radio

mesh

interface-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:

- Wireless Controller — RFS4011

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 with connectivity to portals and connects through them)
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
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)
preferred-peer <1-6> <MAC>	Configures a preferred peer device • <1-6> – Configures the priority at which the peer node will be added • <MAC> – Sets the MAC address of the preferred peer device (Ethernet MAC of either an AP or a wireless controller 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

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#mesh client

rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
 interface radio1
  description primary\ radio\ to\ use
  channel 1
```

```
data-rates custom basic-mcs0-7
mesh client
beacon period 50
beacon dtim-period bss 1 2
--More--
```

Related Commands:

no	Disables a selected radio's mesh mode operation

meshpoint

interface-radio instance

Maps an existing meshpoint to this radio

Supported in the following platforms:

- Wireless Controller — RFS4011

Syntax:

```
mesh <MESHPOINT-NAME> {bss <1-8>}
```

Parameters

```
mesh <MESHPOINT-NAME> {bss <1-8>}
```

meshpoint <MESHPOINT-NAME>	Maps a meshpoint to this radio. Specify the meshpoint name.
bss <1-8>	Optional. Specifies the BSS number on the radio where this meshpoint is mapped • <1-8> – Specify the BSS number from 1 - 8.

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#meshpoint test
```

Related Commands:

no	Disables meshpoint on the selected radio

no

interface-radio instance

Negates a command or resets settings to their default. When used in the config Brocade Mobility RFS4000 radio Interface mode, the no command disables or resets radio interface settings.

Supported in the following platforms:

- Wireless Controller — RFS4011

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

```
rfs4000-880DA7(config-profile-default-rfs4000-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
  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)
  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-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 (2347)
  shutdown                 Re-enable the selected interface
  sniffer-redirect         Disable capture and redirection of packets
  stbc                     Configure Space-Time Block Coding (STBC) parameters
  txbf                     Configure Transmit Beamforming (txbf) parameters
  use                      Set setting to use
  wireless-client          Configure wireless client related parameters
```

```
  wlan                      Disable a wlan from this radio

  service                   Service Commands

rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#
```

The following example shows the radio interface settings before execution of the ‘no’ commands:

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
 interface radio1
  description primary\ radio\ to\ use
  channel 1
  data-rates custom basic-mcs0-7
  mesh client
  beacon period 50
  beacon dtim-period bss 1 2
  beacon dtim-period bss 2 20
  beacon dtim-period bss 3 2
  beacon dtim-period bss 4 2
  beacon dtim-period bss 5 2
  beacon dtim-period bss 6 2
  beacon dtim-period bss 7 2
  beacon dtim-period bss 8 2
  beacon dtim-period bss 9 2
  beacon dtim-period bss 10 2
  beacon dtim-period bss 11 2
  beacon dtim-period bss 12 2
  beacon dtim-period bss 13 2
  beacon dtim-period bss 14 2
  beacon dtim-period bss 15 2
  beacon dtim-period bss 16 2
  antenna-gain 12.0
  guard-interval long
  aggregation ampdu tx-only
  aeroscout mac 11-22-33-44-55-66
  antenna-mode 1xALL
  antenna-diversity
  max-clients 100
  airtime-fairness prefer-ht weight 6
  lock-rf-mode
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#

rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#no beacon
dtim-period
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#no channel
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#no antenna-gain
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#no description
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#no antenna-mode
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#no max-clients
```

The following example shows the radio interface settings after execution of the ‘no’ commands:

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
 interface radio1
  data-rates custom basic-mcs0-7
  mesh client
  beacon period 50
  guard-interval long
```

```
  aggregation ampdu tx-only
  aeroscout mac 11-22-33-44-55-66
  antenna-diversity
  airtime-fairness prefer-ht weight 6
  lock-rf-mode
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#
```

Related Commands:

aeroscout	Enables Aeroscout Multicast packet forwarding
aggregation	Configures 802.11n aggregation parameters
airtime-fairness	Enables equal access for wireless clients based on their airtime usage
antenna-diversity	Transmits antenna diversity for non-11n transmit rates
antenna-downtilt	Enables the *Advanced Element Panel Technology* (ADEPT) antenna mode
antenna-gain	Configures the radio antenna gain
antenna-mode	Configures the radio antenna mode (the number of transmit and receive antennas)
beacon	Configure beacon parameters
channel	Configures a radio channel of operation
data-rates	Configures 802.11 data rates on a radio
description	Defines a radio's description
dfs-rehome	Reverts to configured home channel once DFS evacuation period expires
dynamic-chain-selection	Enables automatic antenna mode selection (single antenna for non-11n transmit rates)
ekahau	Enables Ekahau multicast packet forwarding
extended-range	Configures a radio's extended range settings (in kilometers)
guard-interval	Configures the 802.11n guard interval
lock-rf-mode	Retains user configured radio RF mode settings
max-clients	Configures the maximum number of wireless clients allowed to associate with a radio
mesh	Enables this radio to operate in the mesh mode
meshpoint	Maps an existing meshpoint to the selected radio
non-unicast	Configures the handling of radio non unicast frames
off-channel-scan	Enables radio off channel scanning parameters
placement	Configures the location where a radio is deployed
power	Configures the radio transmit power
preamble-short	Enables the use of short preamble on a radio
probe-response	Configures transmission parameters for probe response frames
radio-share-mode	Configures the radio tap mode of operation for this radio
rf-mode	Configures the radio RF mode
rifs	Configures radio RIFS parameters
rts-threshold	Configures the radio *Request to Send* (RTS) threshold value
shutdown	Terminates or shutsdown a radio interface
sniffer-redirect	Captures and redirects packets to an IP address running a packet capture/analysis tool

stbc	Configures a radio's *Space Time Block Coding* (STBC) mode
use	Enables the use of an association ACL policy and a radio QoS policy by an interface
wireless-client	Configures wireless client parameters
wlan	Enables a WLAN on this radio
service	Service commands are used to view and manage system configuration

non-unicast

interface-radio instance

Configures the management of non unicast frames. This command enables the forwarding of multicast and broadcast frames.

Supported in the following platforms:

- Wireless Controller — RFS4011

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 the support of 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
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 the support of 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 the support of non unicast frames
tx-rate	Configures the transmission data rate for broadcast and multicast frames
bss <1-16>	Overrides the default on a specific 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

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#non-unicast queue
bss 2 3

rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#non-unicast tx-rate
bss 1 dynamic-all

rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
 interface radio1
  data-rates custom basic-mcs0-7
  mesh client
  beacon period 50
  guard-interval long
  aggregation ampdu tx-only
  aeroscout mac 11-22-33-44-55-66
  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
--More--
```

Related Commands:

no	Resets the handling of non unicast frames to its default

off-channel-scan

interface-radio instance

Enables selected radio's off channel scanning parameters

Supported in the following platforms:

- Wireless Controller — RFS4011

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.
scan-interval <2-100>	Optional. Configures the scan interval in dtims • <2-100> – Specify a value from 2 - 100.

`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 *TaZmen Sniffer Protocol* (TZSP) (use with WireShark other tools) before redirecting • <IP> – Specify the destination device IP address.

Example

```
rfs4000-880DA7(config-profile-default-Brocade Mobility
RFS4000-if-radio1)#off-channel-scan channel-list 2.4GHz 1

rfs4000-880DA7(config-profile-default-Brocade Mobility
RFS4000-if-radio1)#show context
 interface radio1
  data-rates custom basic-mcs0-7
  mesh preferred-peer 2 11-22-33-44-55-66
  beacon period 50
  off-channel-scan channel-list 2.4GHz 1
  aggregation ampdu tx-only
  aeroscout mac 11-22-33-44-55-66
  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 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
  antenna-mode 2x2
  antenna-diversity
  max-clients 100
  airtime-fairness prefer-ht weight 6
  lock-rf-mode
rfs4000-880DA7(config-profile-default-Brocade Mobility RFS4000-if-radio1)#
```

Related Commands:

no	Disables radio off channel scanning

placement

interface-radio instance

Defines the location where the radio is deployed

Supported in the following platforms:

- Wireless Controller — RFS4011

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

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#placement outdoor

rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
 interface radio1
  data-rates custom basic-mcs0-7
  placement outdoor
  mesh client
  beacon period 50
  off-channel-scan channel-list 2.4GHz 1
  guard-interval long
  aggregation ampdu tx-only
  aeroscout mac 11-22-33-44-55-66
  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--
```

Related Commands:

no	Resets a radio's deployment location

power

interface-radio instance

Configures the transmit power on this radio

Supported in the following platforms:

- Wireless Controller – RFS4011

Syntax:

```
power [<1-27>|smart]
```

Parameters

```
power [<1-27>|smart]
```

power	Configures a radio's transmit power

<1-27>	Transmits power in dBm (actual power could be lower based on regulatory restrictions)
smart	Smart RF determines the optimum power

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#power 12

rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
 interface radio1
  power 12
  data-rates custom basic-mcs0-7
  placement outdoor
  mesh client
  beacon period 50
  off-channel-scan channel-list 2.4GHz 1
  guard-interval long
  aggregation ampdu tx-only
  aeroscout mac 11-22-33-44-55-66
  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--
```

Related Commands:

no	Resets a radio's transmit power

preamble-short

interface-radio instance

Enables the use of short preamble on this radio

Supported in the following platforms:

- Wireless Controller — RFS4011

Syntax:

```
preamble-short
```

Parameters

None

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#preamble-short
```

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
 interface radio1
  power 12
  data-rates custom basic-mcs0-7
  placement outdoor
  mesh client
  beacon period 50
  off-channel-scan channel-list 2.4GHz 1
  preamble-short
  guard-interval long
  aggregation ampdu tx-only
  aeroscout mac 11-22-33-44-55-66
  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--
```

Related Commands:

no	Disables the use of short preamble on a radio

probe-response

interface-radio instance

Configures transmission parameters for probe response frames.

Supported in the following platforms:

- Wireless Controller — RFS4011

Syntax:

```
probe-response [rate|retry]
probe-response rate [follow-probe-request|highest-basic|lowest-basic]
```

Parameters

```
probe-response retry
```

probe-response	Configures probe response frame transmission parameters
retry	Retransmits the probe response if no acknowledgement is received from the client

```
probe-response rate [follow-probe-request|highest-basic|lowest-basic]
```

probe-response	Configures probe response frame transmission parameters
rate	Configures the transmitted probe response data rates
follow-probe-request	Transmits probe responses at the same rate as the received requests

highest-basic	Uses the highest configured basic rate
lowest-basic	Uses the lowest configured basic rate

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#probe-response rate
follow-probe-request
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#
```

Related Commands:

no	Resets transmission parameters for probe response frames

radio-share-mode

interface-radio instance

Configures the mode of operation, for this radio, as radio-share

Supported in the following platforms:

- Wireless Controller — Brocade Mobility RFS4000

Syntax:

```
radio-share-mode [inline|off|promiscuous]
```

Parameters

```
radio-share-mode [inline|off|promiscuous]
```

radio-share-mode	Configures the radio share mode
inline	Enables sharing of WLAN packets serviced by this radio (matching the BSSID of the radio)
off	Disables radio share (no packets shared with WIPS sensor module)
promiscuous	Enables the sharing of packets received in promiscuous mode without filtering based on BSSID

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#radio-share-mode
promiscuous

rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
 interface radio1
  power 12
  data-rates custom basic-mcs0-7
  placement outdoor
  mesh client
  beacon period 50
  off-channel-scan channel-list 2.4GHz 1
  preamble-short
  guard-interval long
  aggregation ampdu tx-only
  aeroscout mac 11-22-33-44-55-66
  non-unicast tx-rate bss 1 dynamic-all
  non-unicast tx-rate bss 2 highest-basic
  ..............................................................
  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
  radio-share-mode promiscuous
  airtime-fairness prefer-ht weight 6
  lock-rf-mode
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#
```

Related Commands:

no	Resets the radio share mode for this radio to its default

rate-selection

interface-radio instance

Sets the rate selection method to standard or opportunistic

NOTE
This feature is not supported on a Brocade Mobility RFS4000model controller.

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 71XX 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)

rf-mode

interface-radio instance

Configures the radio's RF mode

Supported in the following platforms:

- Wireless Controller — RFS4011

Syntax:

```
rf-mode [2.4GHz-wlan|4.9GHz-wlan|5GHz-wlan|sensor]
```

Parameters

```
rf-mode [2.4GHz-wlan|4.9GHz-wlan|5GHz-wlan|sensor]
```

rf-mode	Configures the radio RF mode
2.4GHz-wlan	Provides WLAN service in the 2.4 GHz band
4.9GHz-wlan	Provides WLAN service in the 4.9 GHz band
5GHz-wlan	Provides WLAN service in the 5.0 GHz band
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

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#rf-mode sensor

rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
 interface radio1
  rf-mode sensor
  placement outdoor
  mesh client
  beacon period 50
  off-channel-scan channel-list 2.4GHz 1
  guard-interval long
  aggregation ampdu tx-only
  aeroscout mac 11-22-33-44-55-66
  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-basicx
  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--
```

Related Commands:

no	Resets the RF mode for a radio to its default (2.4 GHz on radio1, 5.0 GHz on radio2, and sensor on radio3)

rifs

interface-radio instance

Configures *Reduced Interframe Spacing* (RIFS) parameters on this radio. In scenarios where frame aggregation is not possible, RIFS is a means of reducing the interframe overhead. RIFS reduces the dead time between frames by specifying an interframe space smaller than the *Short Interframe Space* (SIFS).

Supported in the following platforms:

- Wireless Controller — RFS4011

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
rx-only	Supports RIFS possession only
tx-only	Supports RIFS transmission only
tx-rx	Supports both RIFS transmission and possession

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#rifs tx-only

rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
 interface radio1
  rf-mode sensor
  placement outdoor
  mesh client
  beacon period 50
  off-channel-scan channel-list 2.4GHz 1
  guard-interval long
  aggregation ampdu tx-only
  rifs tx-only
  aeroscout mac 11-22-33-44-55-66
  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--
```

Related Commands:

no	Disables radio RIFS parameters

rts-threshold

interface-radio instance

Configures the RTS threshold value on this radio

Supported in the following platforms:

- Wireless Controller — RFS4011

Syntax:

```
rts-threshold <1-2347>
```

Parameters

```
rts-threshold <1-2347>
```

<1-2347>	Specify the RTS threshold value from 1 - 2347 bytes

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#rts-threshold 100

rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
 interface radio1
  rf-mode sensor
  placement outdoor
  mesh client
  beacon period 50
  rts-threshold 100
  off-channel-scan channel-list 2.4GHz 1
  guard-interval long
  aggregation ampdu tx-only
  rifs tx-only
  aeroscout mac 11-22-33-44-55-66
  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--
```

Related Commands:

no	Resets a radio's RTS threshold to its default (2347)

shutdown

interface-radio instance

Terminates or shuts down a radio interface

Supported in the following platforms:

- Wireless Controller — RFS4011

Syntax:

```
shutdown
```

Parameters

None

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#shutdown
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#
```

Related Commands:

no	Enables a disabled radio interface

sniffer-redirect

interface-radio instance

Captures and redirects packets to an IP address running a packet capture/analysis tool

Supported in the following platforms:

- Wireless Controller — RFS4011

Syntax:

```
sniffer-redirect [omnipeek|tzsp] <IP> channel [1|1+|10|10-|100--------165]
```

Parameters

```
sniffer-redirect [omnipeek|tzsp] <IP> channel [1|1+|10|10---------165]
```

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 (use with WireShark and other tools)

<IP>	Specify the IP address of the device running the capture/analysis tool
[1|1+|10|10-|100|---------165]	Specify the channel to capture packets • 1 – Channel 1 in 20 MHz • 1+ – Channel 1 as primary, Channel 5 as extension • 10 – Channel 10 in 20 MHz • 10- – Channel 10 as primary, Channel 6 as extension • 100 – Channel 100 in 20 MHz

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#sniffer-redirect
omnipeek 172.16.10.1 channel 1

rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
 interface radio1
  rf-mode sensor
  placement outdoor
  mesh client
  beacon period 50
  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 mac 11-22-33-44-55-66
  non-unicast tx-rate bss 1 dynamic-all
  non-unicast tx-rate bss 2 highest-basic
--More--
```

Related Commands:

no	Disables capture and redirection of packets

stbc

interface-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).

Supported in the following platforms:

- Access Points — Brocade Mobility 6511 Access Point

NOTE
This feature is not supported on a RFS4011 model controller.

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-radio instance

The `use` command enables the use of an association ACL policy and a radio QoS policy by this radio interface

Supported in the following platforms:

- Wireless Controller — RFS4011

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.
radio-qos-policy	Uses a specified radio QoS policy with this radio interface • <RADIO-QoS-POLICY-NAME> – Specify the radio QoS policy name

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#use radio-qos-policy
default
```

Related Commands:

no	Disables the use of the specified association ACL policy and radio QoS policy

wireless-client

interface-radio instance

Configures wireless client parameters on this radio

Supported in the following platforms:

- Wireless Controller — RFS4011

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. Advertises in the Symbol/Brocade information element (176) • symbol-ie – Advertises in the Symbol/Brocade information element (176) • 802.11d – Optional. Advertises in the IEEE 802.11d country information element

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#wireless-client
tx-power 20

rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
 interface radio1
  rf-mode sensor
  placement outdoor
  mesh client
  beacon period 50
  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
  sniffer-redirect omnipeek 172.16.10.1 channel 1
  aeroscout mac 11-22-33-44-55-66
  non-unicast tx-rate bss 1 dynamic-all
  ..........................................................
--More--
```

Related Commands:

no	Resets the transmit power indicated to wireless clients

wlan

interface-radio instance

Enables a WLAN on this radio

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000

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 to the WLAN • <1-8> – Specify the BSS number from 1 - 8. • primary – Optional. Uses the WLAN as the primary WLAN when multiple WLANs exist on the BSS • primary – Optional. Uses the WLAN as the primary WLAN when multiple WLANs exist on the BSS

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#wlan TestWLAN
primary

rfs4000-880DA7(config-profile-default-rfs4000-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
  non-unicast tx-rate bss 7 highest-basic
  non-unicast tx-rate bss 8 highest-basic
  non-unicast tx-rate bss 9 highest-basic
--More--
```

Related Commands:

no	Disables a WLAN on a radio

23

Chapter

L2TPV3-Policy

24

In this chapter

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 teardown 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.

L2TP V3 enables supported controllers and access points to create tunnels for transporting Ethernet frames to and from bridge VLANs and physical ports. L2TP V3 tunnels can be defined between Brocade Mobility devices and other vendor devices supporting the L2TP V3 protocol.

Multiple pseudowires can be created within an L2TP V3 tunnel. Brocade Mobility supported access points support an Ethernet VLAN pseudowire type exclusively.

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 L2TP V3 tunnels can be defined between tunnel end points. Each tunnel can have one or more L2TP V3 sessions. Each tunnel session corresponds to one pseudowire. An L2TP V3 control connection (a L2TP V3 tunnel) needs to be established between the tunneling entities before creating a session.

For optimal pseudowire operation, both the L2TP V3 session originator and responder need to know the psuedowire type and identifier. These two parameters are communicated during L2TP V3 session establishment. An L2TP V3 session created within an L2TP V3 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 L2TP V3 session. If a L2TP V3 session is down, the pseudowire associated with it must be shut down. The L2TP V3 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*.

24

This chapter is organized into the following sections:

- *l2tpv3-policy-commands*
- *l2tpv3-tunnel-commands*
- *l2tpv3-manual-session-commands*

l2tpv3-policy-commands

Use the (config) instance to configure L2TPV3 policy parameters. To navigate to the L2TPV3 policy instance, use the following commands:

```
rfs7000-37FABE(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 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)#
```

Table 64 summarizes L2TPV3 policy configuration commands.

TABLE 64 L2TPV3-Tunnel-Policy-Config Commands

Command	Description	Reference
cookie-size	Configures the cookie field size for each L2TPV3 data packet	*page 24-943*
failover-delay	Configures the L2TPV3 tunnel failover delay in seconds	*page 24-944*
force-12-path-recovery	Enables the forced detection of servers and gateways behind the L2TPV3 tunnel	*page 24-945*
hello-interval	Configures the interval, in seconds, between L2TPV3 “Hello” keep-alive messages exchanged in the L2TPV3 control connection	*page 24-946*
no	Negates or reverts L2TPV3 tunnel commands	*page 24-946*
reconnect-attempts	Configures the maximum number of retransmissions for signalling messages	*page 24-948*
reconnect-interval	Configures the interval, in seconds, between successive attempts to re-establish a failed tunnel connection	*page 24-948*
retry-attempts	Configures the maximum number of retransmissions for signalling messages	*page 24-949*
retry-interval	Configures the interval, in seconds, before initiating a retransmission of any L2TPV3 signalling message	*page 24-950*
rx-window-size	Configures the number of signalling messages received without sending an acknowledgement	*page 24-951*
tx-window-size	Configures the number of signalling messages transmitted without receiving an acknowledgement	*page 24-951*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes the system’s running configuration to memory or terminal	*page 5-310*

cookie-size

l2tpv3-policy-commands

Configures the size of the cookie field present in each L2TPV3 data packet. A tunnel 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.

Supported in the following platforms:

- Access Points — Brocade Mobility 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 fail-over 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 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
no
[cookie-size|fail-over|hello-interval|reconnect-attempts|reconnect-interval|
          retry-attempts|retry-interval|rx-window-size|tx-window-size]
```

Parameters

```
no [cookie-size|hello-interval|reconnect-attempts|reconnect-interval|
      retry-attempts|retry-interval|rx-window-size|tx-window-size]
```

no cookie-size	Resets the cookie-field size to default (0 - no cookie field present in each L2TPV3 data packet)
no fail-over	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 acknowledgement to default (10 packets)
no tx-window-size	Resets the number of packets transmitted without receiving an acknowledgement 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)#

rfs7000-37FABE(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 acknowledgement
tx-window-size	Configures the number of packets transmitted without receiving an acknowledgement

reconnect-attempts

l2tpv3-policy-commands

Configures the maximum number of attempts to reestablish a tunnel connection

Supported in the following platforms:

- Access Points — Brocade Mobility 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
reconnect-attempts <0-8>
```

Parameters

```
reconnect-attempts <0-8>
```

reconnect-attempts <0-250>	Configures the maximum number of attempts to reestablish 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 successive attempts to re-establish a failed tunnel connection

Supported in the following platforms:

- Access Points — Brocade Mobility 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 retransmissions for signalling messages. Use this command to specify how many retransmission cycles occur before determining the peer is not reachable.

Supported in the following platforms:

- Access Points — Brocade Mobility 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
retry-attempts <1-10>
```

Parameters

```
retry-attempts <1-10>
```

retry-attempts <1-10>	Configures the maximum number of retransmissions for 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 for signalling messages to default (5 attempts)

retry-interval

l2tpv3-policy-commands

Configures the interval, in seconds, before initiating a retransmission of a L2TPV3 signalling message

Supported in the following platforms:

- Access Points — Brocade Mobility 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
retry-interval <1-250>
```

Parameters

```
retry-interval <1-250>
```

retry <1-250>	Configures the interval before initiating a retransmission of a L2TPV3 signalling message. 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 interval before initiating a retransmission of a L2TPV3 signalling message to default (5 seconds)

rx-window-size

l2tpv3-policy-commands

Configures the number of signalling packets received without sending an acknowledgement

Supported in the following platforms:

- Access Points — Brocade Mobility 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 acknowledgement. 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 acknowledgement to default (10 packets)

tx-window-size

l2tpv3-policy-commands

Configures the number of signalling packets transmitted without receiving an acknowledgement

Supported in the following platforms:

- Access Points — Brocade Mobility 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 acknowledgement. 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 acknowledgement to default (10 packets)

l2tpv3-tunnel-commands

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:

```
rfs7000-37FABE(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 sepcific 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)#
```

Table 65 summarizes L2TPV3 tunnel configuration commands.

TABLE 65 L2TPV3-Tunnel-Config Commands

Command	Description	Reference
establishment-criteria	Configures L2TPV3 tunnel establishment criteria	*page 24-953*
hostname	Configures tunnel specific local hostname	*page 24-954*
local-ip-address	Configures the tunnel's IP address	*page 24-955*
mtu	Configures the tunnel's *Maximum Transmission Unit* (MTU) size	*page 24-956*
no	Negates or reverts L2TPV3 tunnel commands	*page 24-956*
peer	Configures the tunnel's peers	*page 24-958*
router-id	Configures the tunnel's local router ID	*page 24-960*
session	Creates/modifies specified L2TPV3 session	*page 24-961*
use	Configures a tunnel to use a specified L2TPV3 tunnel policy	*page 24-962*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes the system's running configuration to memory or terminal	*page 5-310*

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 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 L2TPV3 tunnel. 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 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 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. 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 setting (always)

hostname

l2tpv3-tunnel-commands

Configures the tunnel's local hostname

Supported in the following platforms:

- Access Points — Brocade Mobility 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 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 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 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
host
name 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 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
router-id [<1-4294967295>|<I>]
```

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 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 name. Maximum of four critical resources can configured for monitoring. 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. 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

Use the (profile-context) instance to configure a L2TPV3 manual session. To navigate to the L2TPV3 manual session configuration mode, use the following command in the profile context:

```
rfs7000-37FABE(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 mannual 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)#
```

Table 66 summarizes L2TPV3 manual session configuration commands.

TABLE 66 L2TPV3-Manual-Session-Config Commands

Command	Description	Reference
local-cookie	Configures the manual session's local cookie field size	*page 24-964*
local-ip-address	Configures the manual session's local source IP address	*page 24-965*
local-session-id	Configures the manual session's local session ID	*page 24-965*
mtu	Configures the MTU size for the manual session tunnel	*page 24-966*

TABLE 66 L2TPV3-Manual-Session-Config Commands

Command	Description	Reference
no	Negates or reverts L2TPV3 manual session commands to default	*page 24-956*
peer	Configures the manual session's peers	*page 24-968*
remote-cookie	Configures the remote cookie for the manual session	*page 24-969*
remote-session-id	Configures the manual session's remote session ID	*page 24-970*
traffic-source	Configures the traffic source tunneled by the manual session	*page 24-971*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes the system's running configuration to memory or terminal	*page 5-310*

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 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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.

Supported in the following platforms:

- Access Points — Brocade Mobility 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

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

Supported in the following platforms:

- Access Points — Brocade Mobility 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 remote session's ID

Supported in the following platforms:

- Access Points — Brocade Mobility 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
remote-session-id <1-4294967295>
```

Parameters

```
remote-session-id <1-4294967295>
```

remote-session-id <1-4294967295>	Configures this manual remote session's 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 remote session's ID

traffic-source

l2tpv3-manual-session-commands

Configures the traffic source tunneled by this session

Supported in the following platforms:

- Access Points — Brocade Mobility 7131 Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

24

Chapter

Router-Mode Commands

25

In this chapter

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. It is based on the shortest first or link-state algorithm that updates the routing table. OSPF driven routing table updates are triggered only when network changes occur and not at predefined intervals. When a host detects a network change, it forwards the information to other hosts on the network. This enables routers to synchronize routing tables.

Use the (config) instance to configure router commands. To navigate to the (config-router-mode) instance, use the following commands:

```
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)#
```

25

router-mode

Table 67 summarizes router configuration commands.

TABLE 67 OSPF-Router Config Commands

Command	Description	Reference
area	Specifies *Open Shortest Path First* (OSPF) enabled interfaces	*page 25-974*
auto-cost	Specifies the reference bandwidth in terms of Mbits per second	*page 25-975*
default-information	Controls the distribution of default information	*page 25-976*
ip	Configures *Internet Protocol* (IP) default gateway priority	*page 25-977*
network	Defines OSPF network settings	*page 25-978*
ospf	Enables OSPF	*page 25-978*
passive	Specifies the configured OSPF interface as passive interface	*page 25-979*
redistribute	Specifies the route types redistributed by OSPF	*page 25-980*
route-limit	Specifies the limit for the number of routes managed by OSPF	*page 25-981*
router-id	Specifies the router ID for OSPF	*page 25-982*
vrrp-state-check	Publishes interface via OSPF based on VVRP status	*page 25-983*
no	Negates a command or sets its defaults	*page 25-983*

area

router-mode

Configures OSPF network areas (OSPF enables interfaces)

OSPF networks consist of routers and links grouped into areas. Each area is identified by an assigned number. 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.

Supported in the following platforms:

- Access Points — Brocade Mobility 71XX 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

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 banwidth

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 71XX 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.

Supported in the following platforms:

- Access Points — Brocade Mobility 71XX 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
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)

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 *Internet Protocol* (IP) default gateway priority

Supported in the following platforms:

- Access Points — Brocade Mobility 71XX 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. 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 71XX 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
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 1.2.3.4/5
area 4.5.6.7

rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#show context
 router ospf
  network 1.2.3.4/24 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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
ospf enable
```

Parameters

```
ospf enable
```

ospf enable	Enables OSPF routing

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 1.2.3.4/24 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

A passive interface receives routing updates, but does not transmit them.

Supported in the following platforms:

- Access Points — Brocade Mobility 71XX 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 1.2.3.4/24 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 71XX 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>	Optional. Specifies the OSPF metric value for redistributed routes. Specify a value from 0 - 16777214.
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 1.2.3.4/24 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 71XX 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.

retry-count <1-32>	Specifies the maximum number of times adjacencies can be suppressed. Each time OSPF gets into an ignore state, a counter is incremented. 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.
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.

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 1.2.3.4/24 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

Supported in the following platforms:

- Access Points — Brocade Mobility 71XX 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

Supported in the following platforms:

- Access Points — Brocade Mobility 71XX 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 71XX 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 1.2.3.4/24 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
referenc
e-bandwidth
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#no network
1.2.3.4/24  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 Mbits per second
default-information	Controls the distribution of default route information
ip	Configures *Internet Protocol* (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 *Virtual Router Redundancy Protocol* (VVRP) status

OSPF-area-mode

router-mode

Use the (config) instance to configure ospf-area commands. To navigate to the (config-router-ospf-area-mode) instance, use the following commands:

```
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#area 1
rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#?
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-0.0.0.1)#
```

Table 68 summarizes OSPF area mode configuration commands.

TABLE 68 OSPF-Area-Mode Commands

Command	Description	Reference
area-type	Configures a particular OSPF area as STUB or NSSA	*page 25-986*
authentication	Specifies the authentication scheme used for the OSPF area	*page 25-987*

TABLE 68 OSPF-Area-Mode Commands

Command	Description	Reference
range	Specifies the routes matching address/mask for summarization	*page 25-988*
no	Negates a command or sets its defaults	*page 25-988*

area-type

OSPF-area-mode

Configures a particular OSPF area as STUB, Totally STUB, NSSA or Totally NSSA

Supported in the following platforms:

- Access Points — Brocade Mobility 71XX 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 *Not So Stubby Area* (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 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

Supported in the following platforms:

- Access Points — Brocade Mobility 71XX 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 a message-digest (MD-5) authentication scheme
simple-password	Configures a 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 that want to participate in the routing domain will 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 an authentication scheme used for an OSPF area

range

OSPF-area-mode

Specifies the routes matching address/mask for summarization

Supported in the following platforms:

- Access Points — Brocade Mobility 71XX 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
172.16.10.2/24

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 172.16.10.2/24
   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

router-mode

Negates a command or set its defaults

Supported in the following platforms:

- Access Points — Brocade Mobility 71XX 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 172.16.10.2/24
   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)#no area-type
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
 172.16.10.2/24

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

25

Chapter

Routing-Policy

26

In this chapter

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 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, routing policies facilitate the provisioning of preferential service to specific traffic.

Use the (config) instance to configure router-policy commands. To navigate to the (config-routing-policy mode) instance, use the following commands:

```
rfs7000-37FABE(config)#routing-policy testpolicy
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

Table 69 summarizes routing policy configuration commands.

TABLE 69 Routing-Policy-Config Commands

Command	Description	Reference
apply-to-local-packets	Enables/disables policy based routing for locally generated packets	*page 26-992*
logging	Enables logging for a specified route map	*page 26-993*
route-map	Creates a route map entry	*page 26-993*
use	Defines default settings to use	*page 26-1000*
no	Negates a command or sets its defaults	*page 26-1000*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
do	Runs commands from the EXEC mode	*page 4-165*
end	Ends and exits current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends current mode and moves to the previous mode	*page 5-277*
help	Displays interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes information to memory or terminal	*page 5-310*

apply-to-local-packets

routing-policy-commands

Enables/disables *policy-based routing* (PBR) for locally generated packets

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 71XX 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 logging for a specified route map

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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. Several route map entries can be configured, each having a unique sequence number. Entries are evaluated according to their sequence number, until a match is made. If no match is made, packets are routed normally.

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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. 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

Table 70 summarizes route-map configuration commands.

TABLE 70 Route-Map-Config Commands

Command	Description	Reference
default-next-hop	Sets the next hop for packets that satisfy the specified match criteria	*page 26-995*
fallback	Configures a fallback to the next destination	*page 26-995*
mark	Marks action for the route map	*page 26-996*

TABLE 70 Route-Map-Config Commands

Command	Description	Reference
match	Sets the match clause configuration for a specified route map	*page 26-997*
next-hop	Sets the next hop for packets that satisfy the specified match criteria	*page 26-998*
no	Negates a command or sets its default	*page 26-999*

default-next-hop

route-map-mode

Sets the next hop for packets that satisfy the specified match criteria

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

Configures a fallback to the next destination. If none of the configured outgoing interfaces and next hops are up, then fallback to the normal destination is configured. If fallback is not configured, the default behavior is to drop the packet.

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 a fallback to destination based routing if no next hop is configured or all are unreachable

mark

route-map-mode

Marks an action for the route map

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 clause configuration for a specified route map

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 name. Specify a VLAN ID from 1 - 4094.
wwan1	Specifies the WAN interface name

`match ip dscp <0-63>`

ip dscp <0-63>	Sets the *Differentiated Services Code Point* (DSCP) match clause. Specify a DS code point value from 0 - 63.

`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 that satisfies the specified match criteria

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 for packets that satisfy the match criteria
[A.B.C.D]	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 300 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
no [default-next-hop|fallback|mark|match|next-hop]
```

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

```
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 that satisfy the specified match criteria
fallback	Configures a fallback to the next destination
mark	Marks an action for the route map
match	Sets the match clause configuration for a specified route map
next-hop	Sets the next hop for packets that satisfies the specified match criteria

use

routing-policy-commands

Uses *Critical Resource Monitoring* (CRM) to monitor link status

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
use critical-resource-monitoring
```

Parameters

```
use critical-resource-monitoring
```

use critical-resource-monitoring	Uses CRM to monitor the status of a link. This determines the status of the next hop in the route map, via the critical resources being monitored. Link monitoring is used for failover to a secondary next hop.

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

route-map-mode

Negates a command or sets its defaults

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
no [apply-to-local-packets|logging|route-map|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

```
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 policy-based routing 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 *Critical Resource Monitoring* (CRM) to monitor the status of a link

26

Chapter

AAA-TACACS-Policy

27

In this chapter

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:

```
RFSSwitch(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

Table 71 summarizes AAA-TACACS policy configuration commands.

TABLE 71 AAA-TACACS-Policy-Config Commands

Command	Description	Reference
accounting	Configures TACACS accounting parameters	*page 27-1004*
authentication	Configures TACACS authentication parameters	*page 27-1006*
authorization	Configures TACACS authorization parameters	*page 27-1008*
no	Negates a command or sets its default	*page 27-1010*

TABLE 71 AAA-TACACS-Policy-Config Commands

Command	Description	Reference
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
do	Runs commands from the EXEC mode	*page 4-165*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug `(config-if)`instance configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes information to memory or terminal	*page 5-310*

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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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
commands	Enables accounting for commands
session	Enables accounting for session start and stop details

	`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 to)
authenticated-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 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 or 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. • 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 attempt. • A value greater than 100 indicates the time gap between two consecutive retries increases with each successive retry attempt.

	`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 • <3-5> – Specify a value from 3 - 5 seconds.
attempts <1-3>	Optional. Specifies the number of times a transmission request is attempted • <1-3> – Specify a value from 1 - 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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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] {(console|ssh|telnet)}`

access-method	Configures access modes for TACACS authentication. The options are: console, SSH, Telnet, 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

`authentication directed-request`

directed-request	Enables user to specify TACACS server to use with `@server' 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. • A value of 100 indicates the time gap between two consecutive retires remains the same irrespective of the number of retries. • A value less than 100 indicates the time gap between two consecutive retries reduces with each successive retry attempt. • A value greater than 100 indicates the time gap between two consecutive retries increases with each successive retry attempt.

`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.
attempts <1-10>	Optional. Indicates the number of retry attempts to make before giving up • <1-10> – Specify a value from 1 -10.

`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

Example

```
rfs7000-37FABE(config-aaa-tacacs-policy-testppolicy)#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 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 an 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. You can optionally configure more than one access method for command authorization.

`authorization allow-privileged-commands`

allow-privileged-commands	Allows privileged commands execution without command authorization

`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 two consecutive TACACS authorization retries • <50-200> – Specify the scaling factor from 50 - 200. • 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 attempt. • A value greater than 100 indicates the time gap between two consecutive retries increases with each successive retry attempt.

```
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.
attempts <1-3>	Optional. Indicates the number of retry attempts to make before giving up • <1-3> – Specify a value from 1 - 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-testppolicy)#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 policy command or sets its default

Supported in the following platforms:

- Access Points — Brocade Mobility 300 Access Point, Brocade Mobility 650 Access Point, Brocade Mobility 6511 Access Point, Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

27

Chapter

Meshpoint 28

In this chapter

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.

meshpoint

Opportunistic Radio Link Adaptation (ORLA), as a part all device's routing engine, provides robust, efficient routing, low hop latency, low routing overhead, high-speed handover, and a scalable mesh network that supports vehicle mounted devices with low hand-over time.

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.

Use the (config) instance to configure meshpoint related configuration commands. To navigate to the meshpoint instance, use the following command:

```
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)#
```

Table 72 summarizes meshpoint configuration commands.

TABLE 72 Meshpoint-Config commands

Command	Description	Reference
allowed-vlans	Configures VLANs allowed on the meshpoint	*page 28-1015*
beacon-format	Configures the beacon format for the meshpoint AP	*page 28-1015*
control-vlan	Configures the VLAN where meshpoint control traffic traverses	*page 28-1016*
data-rates	Configures the data rates supported per frequency band	*page 28-1017*
description	Configures a human friendly description for this meshpoint	*page 28-1020*
meshid	Configures a unique ID for this meshpoint	*page 28-1020*
neighbor	Configures the neighbor inactivity time out for this meshpoint	*page 28-1021*
no	Negates a command or reverts settings to their default	*page 28-1022*
root	Configures a meshpoint as the root meshpoint	*page 28-1025*
security-mode	Configures the security mode on the meshpoint.	*page 28-1025*
service	Allows only 802.11n capable neighbors to create a mesh connection	*page 28-1026*
shutdown	Shuts down the meshpoint	*page 28-1027*
use	Configures a QoS policy for use with this meshpoint	*page 28-1028*
wpa2	Configures WPA2 encryption settings	*page 28-1028*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
do	Runs commands from the EXEC mode	*page 4-165*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug system configurations	*page 5-283*
show	Displays running system information	*page 6-315*
write	Writes information to memory or terminal	*page 5-310*

allowed-vlans

meshpoint

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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. When provided with out any parameters, the VLAN(s) is added to the list of allowed VLANs. A range of VLANs can also be added. Use this command to add VLANs to a new meshpoint.
add <VLAN>	Adds a single VLAN or a range of VLANs to the list of allowed VLANs.
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

Configures the beacon 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 71XX Access Point

Syntax:

```
beacon-format [access-point|mesh-point]
```

Parameters

```
beacon-format [access-point|mesh-point]
```

beacon-format	Configures how a mesh capable BR71XX acts in a mesh network
access-point	The BR71XX acts as an access point
mesh-point	The BR71XX acts as a meshpoint (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

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

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

Configures individual data rates for the 2.4 GHz and 5.0 GHz frequency bands

Supported in the following platforms:

- Access Points — Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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
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 *Modulation and Coding Scheme* (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 802.11n 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
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 *Modulation and Coding Scheme* (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

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
meshid <MESH-SSID>
```

Parameters

```
meshid <MESH-SSID>
```

meshid	Configures a unique *Service Set Identifier* (SSID) for the meshpoint
<MESH-SSID>	The unique SSID configured for this meshpoint The mesh SSID is case sensitive and should not exceed 32 characters.

Example

```
rfs7000-37FABE(config-meshpoint-test)#meshid TesingMeshPoint

rfs7000-37FABE(config-meshpoint-test)#show context
meshpoint test
 description "This is an example of a meshpoint description"
 meshid TesingMeshPoint
 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

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
neighbor inactivity-timeout <60-86400>
```

Parameters

```
neighbor inactivity-timeout <60-86400>
```

neighbor inactivity-timeout <60-86400>	Configures the neighbor inactivity timeout in seconds • <60-86400> – Specify a value from 60 - 86400 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 TesingMeshPoint
 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

Negates meshpoint commands or resets their values to default

Supported in the following platforms:

- Access Points — Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
no [allowed-vlans|beacon-format|control-vlan|description|meshid|root|
          security-mode|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-mode|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
```

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 use of a meshpoint QoS with this meshpoint.

```
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 TesingMeshPoint
 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 exampleutions
 wpa2 key-rotation unicast 1200
 wpa2 key-rotation broadcast 600
 root
```

```
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 exampleutions
 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 exampleutions
 wpa2 key-rotation unicast 1200
 wpa2 key-rotation broadcast 600
 no root
rfs7000-37FABE(config-meshpoint-test)#
```

Related Commands:

allowed-vlans	Configures 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

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
root
```

Parameters

None

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 TesingMeshPoint
 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

Configures the security mode for this meshpoint

Supported in the following platforms:

- Access Points — Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

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 TesingMeshPoint
 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

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 TesingMeshPoint
 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 exampleutions
 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

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

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*.

Supported in the following platforms:

- Access Points — Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

Syntax:

```
use meshpoint-qos-poicy <MESHPOINT-QOS-POLICY-NAME>
```

Parameters

```
use meshpoint-qos-poicy <MESHPOINT-QOS-POLICY-NAME>
```

use meshpoint-qos-policy	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 TesingMeshPoint
 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 an associated meshpoint QoS policy from this meshpoint
meshpoint-qos-policy	Creates and configures a meshpoint QoS policy

wpa2

meshpoint

This command sets the key rotation duration and sets the pre shared keys.

Supported in the following platforms:

- Access Points — Brocade Mobility 71XX Access Point

- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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.
unicast	Configures key rotation interval for unicast packets
<30-86400>	Configures key rotation interval from 30 - 86400 seconds

```
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 exampleutions

rfs7000-37FABE(config-meshpoint-test)#show context
meshpoint test
 description "This is an example of a meshpoint description"
 meshid TesingMeshPoint
 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 exampleutions
 wpa2 key-rotation unicast 1200
 wpa2 key-rotation broadcast 600
 root
```

Related Commands:

no	Resets configuration for PSK and key rotation for this meshpoint.

28

meshpoint-qos-policy

A meshpoint QoS policy defines a set of parameters that defines the *Quality of Service* (QoS). QoS provides a mechanism to provide different priority to different applications, users, data, or to guarantee a certain performance level to traffic flowing in the network.

To create a meshpoint, see *meshpoint*. A meshpoint QoS policy is created from the (config) instance. To create a meshpoint QoS policy use the following command:

meshpoint-qos-policy <POLICYNAME>

```
rfs7000-37FABE(config)#meshpoint-qos-policy test
rfs7000-37FABE(config-meshpoint-qos-policy-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)#
```

Table 73 summarizes the mespoint-qos-policy configuration commands.

TABLE 73 Meshpoint-QoS-Policy Config Commands

Command	Description	Reference
accelerated-multicast	Configures accelerated multicast parameters	*page 28-1031*
no	Negates a command or reverts settings to their default	*page 28-1032*
rate-limit	Configures the rate limits for this QoS policy	*page 28-1033*
clrscr	Clears the display screen	*page 5-275*
commit	Commits (saves) changes made in the current session	*page 5-276*
do	Runs commands from the EXEC mode	*page 4-165*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 4-175*
exit	Ends the current mode and moves to the previous mode	*page 5-277*
help	Displays the interactive help system	*page 5-277*
revert	Reverts changes to their last saved configuration	*page 5-283*
service	Invokes service commands to troubleshoot or debug system configurations	*page 5-283*

TABLE 73 Meshpoint-QoS-Policy Config Commands

Command	Description	Reference
show	Displays running system information	*page 6-315*
write	Writes information to memory or terminal	*page 5-310*

accelerated-multicast

meshpoint-qos-policy

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 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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>	The IP address of the multicast stream to be accelerated
autodetect	Lets the system automatically detect multicast streams to be accelerated
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
```

Related Commands:

no	Resets configuration for accelerated multicast for this meshpoint QoS policy

no

meshpoint-qos-policy

Negates the commands for meshpoint QoS policy or resets their values to their default

Supported in the following platforms:

- Access Points — Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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

`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.

```
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 threshold (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

Configures the rate limiting of traffic on a per meshpoint or per neighbor basis

Supported in the following platforms:

- Access Points — Brocade Mobility 71XX Access Point
- Wireless Controllers — Brocade Mobility RFS4000, Brocade Mobility RFS6000, Brocade Mobility RFS7000

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 a meshpoint
neighbor	Configures rate limit parameters for neighboring meshpoint devices
from-air	Configures rate limit value for traffic from the wireless neighbor to the network.
to-air	Configures rate limit value 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 in the range 2 - 1024 kb.
rate <50-1000000>	Optional. Configures the maximum traffic rate in kilobytes. Set a value in the range 50 - 1000000 kb.

`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 limit value 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>	Configures the threshold for low priority traffic. Set a value in % of max burst size.
best-effort <0-100>	Configures the threshold for best effort traffic. Set a value in % of max burst size.
video <0-100>	Configures the threshold for video traffic. Set a value in % of max burst size.
voice <0-100>	Configures the threshold for voice traffic. Set a value in % of max burst size.

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
```

Related Commands:

no	Resets traffic rate limit settings for this meshpoint QoS policy

Other meshpoint commands

Table 74 lists commands related to meshpoint configuration and setup.

TABLE 74 Other Meshpoint-Related Commands

Command	Description	Reference
meshpoint-device	Configures an BR71XX as a meshpoint device.	*page 28-1035*
monitor	Enables critical resource down event monitoring	*page 28-1036*
no	Negates commands for a meshpoint device or resets values to default	*page 28-1039*
preferred	Configures the preferred path parameters for this meshpoint device	*page 28-1037*
root	Configures this meshpoint device as the root meshpoint	*page 28-1038*

meshpoint-device

Other meshpoint commands

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 71XX 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 wireless 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 — AP622, Brocade Mobility 650 Access Point, Brocade Mobility 71XX 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 BR71XXTestProfile
rfs7000-37FABE(config-profile-BR71XXTestProfile)#meshpoint-device test
rfs7000-37FABE(config-profile-BR71XXTestProfile-meshpoint-test)#
```

```
rfs7000-37FABE(config-profile-BR71XXTestProfile-meshpoint-test)#?
Mesh Point Device Mode commands:
  monitor    Event Monitoring
  no         Negate a command or set its defaults
  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-BR71XXTestProfile-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:
  monitor    Event Monitoring
  no         Negate a command or set its defaults
  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)#?
```

Related Commands:

monitor	Enables monitoring of critical resources and primary port links
preferred	Configures the preferred path parameters
root	Configures this meshpoint device as a root

monitor

meshpoint-device

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 650 Access Point, Brocade Mobility 71XX 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-BR71XXTestProfile-meshpoint-test)#monitor
critical-resource action no-root

rfs7000-37FABE(config-profile-BR71XXTestProfile-meshpoint-test)#show context
 meshpoint-device test
  name test
  monitor critical-resource action no-root
rfs7000-37FABE(config-profile-BR71XXTestProfile-meshpoint-test)#
```

Related Commands:

no	Disables monitoring of critical resource and primary port links.

preferred

meshpoint-device

Configures the preferred path parameters for this meshpoint device

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 71XX Access Point

Syntax:

```
preferred [neighbor <MAC>|root <MAC>|interface [2.4GHz|5GHz]]]
```

Parameters

```
preferred [neighbor <MAC>|root <MAC>|interface [2.4GHz|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|5GHz]	Sets the preferred interface to use

Example

```
rfs7000-37FABE(config-profile-BR71XXTestProfile-meshpoint-test)#preferred
neighbor
11-22-33-44-55-66

rfs7000-37FABE(config-profile-BR71XXTestProfile-meshpoint-test)#preferred
root
22-33-44-55-66-77

rfs7000-37FABE(config-profile-BR71XXTestProfile-meshpoint-test)#preferred
interface 5GHz

rfs7000-37FABE(config-profile-BR71XXTestProfile-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-BR71XXTestProfile-meshpoint-test)#
```

Related Commands:

no	Removes the configuration of preferred paths for this meshpoint device

root

meshpoint-device

Configures this meshpoint device 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 650 Access Point, Brocade Mobility 71XX Access Point

Syntax:

```
root
```

Parameters

None

Example

```
rfs7000-37FABE(config-profile-BR71XXTestProfile-meshpoint-test)#root

rfs7000-37FABE(config-profile-BR71XXTestProfile-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-BR71XXTestProfile-meshpoint-test)#
```

Related Commands:

no	Removes the configuration of this meshpoint device as a root meshpoint

no

meshpoint-device

Negates the commands for a meshpoint device or resets values to default

Supported in the following platforms:

- Access Points — Brocade Mobility 650 Access Point, Brocade Mobility 71XX Access Point

Syntax:

```
no [monitor|preferred|root]

no monitor [critical-resource|primary-port-link-loss]
no root
no preferred [interface|root|neighbor]
```

Parameters

```
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 root
```

no root	Removes the configuration of this meshpoint device as 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-BR71XXTestProfile-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-BR71XXTestProfile-meshpoint-test)#

rfs7000-37FABE(config-profile-BR71XXTestProfile-meshpoint-test)#no monitor
critical-resource
rfs7000-37FABE(config-profile-BR71XXTestProfile-meshpoint-test)#no preferred
neighbor
rfs7000-37FABE(config-profile-BR71XXTestProfile-meshpoint-test)#no root
```

```
rfs7000-37FABE(config-profile-BR71XXTestProfile-meshpoint-test)#no preferred
interface

rfs7000-37FABE(config-profile-BR71XXTestProfile-meshpoint-test)#show context
 meshpoint-device test
  name test
  no root
  preferred root 22-33-44-55-66-77
rfs7000-37FABE(config-profile-BR71XXTestProfile-meshpoint-test)#
```

Related Commands:

monitor	Enables monitoring of critical resources and primary port links
preferred	Configures the preferred path parameters
root	Configures this meshpoint device as a root

Chapter

29 Firewall Logging

In this chapter

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:

```
rfs7000-81916A(config)#May 07 11:09:00 2012: USER: cfgd: deleting session 4
rfs7000-81916A(config)#
rfs7000-81916A(config)#May 07 11:09:17 2012: USER: cfgd: deleting session 5
```

The date format is Month <MMM> Date <DD> Time <HH:MM:SS> Year <YYYY>

```
Month is May
Date is 07
Time is 11:09:00
Year is 2012
```

To generate a date log, enable logging

For example, the following command has to be executed:

```
rfs7000-37FABE#clock set 11:09:17 07 May 2012
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

```
May 07 11:10:17 2012: %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 May 07
Time is 11:10:17
Year is 2012
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

May 07 11:10:19 2012: %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

May 07 11:14:31 2012: %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

May 07 11:57:43 2012: %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

May 07 11:58:48 2012: %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:

May 07 12:00:00 2012: %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:

May 07 12:00:07 2012: %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:

May 07 12:00:25 2012: %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:

May 07 12 01:00:24 2012: %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:

May 07 12:03:00 2012: %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:

May 07 12:04:06 2012: %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:

May 07 12:05:00 2012: %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:

May 07 12:06:00 2012: %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:

May 07 12:07:00 2012: %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:

May 07 12:10:11 2012: %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:

May 07 12:11:50 2012: %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

May 07 12:12:00 2012: %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:

May 07 12:15:21 2012: %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:

May 07 12:16:50 2012: %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.

May 07 12:16:55 2012: %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:

May 07 12:20:30 2012: %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.

May 07 12:22:49 2012: %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. May 19 20:10:09 2010: %NSM-4-IFUP: Interface vlan2 is up

May 07 12:25:09 2012: KERN: vlan2: add 01:00:5e:00:00:01 mcast address to master interface.

May 07 12:25:09 2012: %NSM-4-IFUP: Interface vlan172 is up

May 07 12:25:09 2012: KERN: vlan172: add 01:00:5e:00:00:01 mcast address to master interface.

May 07 12:25:09 2012: %PM-6-PROCSTART: Starting process "/usr/sbin/lighttpd"

May 07 12:25:09 2012: %FILEMGMT-5-HTTPSTART: lighttpd started in external mode with pid 0

May 07 12:25:09 2012: %DAEMON-3-ERR: dhcrelay: interface allocate : vlan1

May 07 12:25:09 2012: %USER-5-NOTICE: FILEMGMT[1086]: FTP: ftp server stopped

May 07 12:25:09 2012: %DAEMON-3-ERR: dhcrelay: interface allocate : vlan1

May 07 12:25:09 2012: %DAEMON-3-ERR: dhcrelay: interface allocate : vlan1

May 07 12:25:09 2012: %DAEMON-3-ERR: dhcrelay: interface allocate : vlan2

May 07 12:25:09 2012: %DOT11-5-COUNTRY_CODE: Country of operation configured to in [India]

May 07 12:25:09 2012: %DIAG-6-NEW_LED_STATE: LED state message AP_LEDS_ON from module DOT11

May 07 12:25:09 2012: %PM-6-PROCSTART: Starting process "/usr/sbin/telnetd"

May 07 12:25:09 2012: %AUTH-6-INFO: sshd[1422]: Server listening on 0.0.0.0 port 22.

dataplane enabled

CCB:21:Firewall enabled

May 07 12:25:09 2012: %KERN-4-WARNING: dataplane enabled.

May 07 12:25:09 2012: %DATAPLANE-5-FWSTARTUP: **Firewall enabled.**

May 07 12:25:09 2012: USER: cfgd: handle_cluster_member_update

May 07 12:25:09 2012: USER: cfgd: ignoring, no cluster configured

May 07 12:25:09 2012: %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 May 07 12:25:33 2012.

Log change in time

```
rfs7000-37FABE#show clock
2012-05-07 12:25:33 UTC
rfs7000-37FABE#
```

rfs7000-37FABE#clock set 12:25:33 07 May 2012

May 07 12:25:33 2012: %[S1]CFGD-6-SYSTEM_CLOCK_RESET: System clock reset, Time: 2012-05-07 12:45:00[S2]

```
rfs7000-37FABE#show clock
May 07 12:45:00 UTC 2012
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 May 2012
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

May 07 12:48:40 2012: %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

May 07 12:48:42 2012: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to wlan
ICSA-testing is getting altered.

IP ACL OUT on WLAN Attach

May 07 12:48:44 2012 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

May 07 12:48:50 2012 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

May 07 12:48:55 2012: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to wlan
ICSA-testing is getting altered.

MAC ACL IN on WLAN Remove

May 07 12:48:572012: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to wlan
ICSA-testing is getting altered.

MAC ACL OUT on WLAN Attach

May 07 12:49:00 2012: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to wlan
ICSA-testing is getting altered.

MAC ACL OUT on WLAN Remove

May 07 12:49:06 2012: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to wlan
ICSA-testing is getting altered.

IP ACL on VLAN Attach

May 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

May 07 12:49:12 2012: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to interface vlan1 is getting altered.

IP ACL on GE Port Attach

May 07 12:49:15 2012: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to interface ge1 is getting altered.

IP ACL on GE Port Remove

May 07 12:49:20 2012: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to interface ge1 is getting altered.

MAC ACL on GE Port Attach

May 07 12:49:22 2012: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to interface ge1 is getting altered.

MAC ACL on GE Port Remove

May 07 12:49:24 2012: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to interface ge1 is getting altered.

IP ACL on Port-Channel Attach

May 07 12:49:30 2012: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to interface
port-channel1 is getting altered.

IP ACL on Port-Channel Remove

May 07 12:50:00 2012: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to interface
port-channel1 is getting altered.

MAC ACL on Port-Channel Attach

May 07 12:50:01 2012: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to interface
port-channel1 is getting altered.

MAC ACL on Port-Channel Remove

May 07 12:50:05 2012: %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 2012: %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:

May 07 20:31:26 2012: %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.

May 07 20:31:31 2012: %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:

May 07 19:57:09 2012: %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.

May 07 19:57:09 2012: %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

May 07 20:37:04 2012: %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.

May 07 20:37:08 2012: %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 5.4.0.0-149320X

Alternate software secondary, version 5.2.0.0-048D

Software fallback feature is enabled

System bootup time (via /proc/uptime) was 126.10 92.38

Please press Enter to activate this console. May 07 20:47:33 2012: %DOT11-5-COUNTRY_CODE: Country of operation configured to in [India]

May 07 20:47:34 2012: %DIAG-6-NEW_LED_STATE: LED state message AP_LEDS_ON from module DOT11

May 07 20:47:34 2012: KERN: vlan1: add 01:00:5e:00:00:01 mcast address to master interface.

May 07 20:47:34 2012: %NSM-4-IFUP: Interface vlan2 is up

May 07 20:47:34 2012: KERN: vlan2: add 01:00:5e:00:00:01 mcast address to master interface.

May 07 20:47:34 2012: %NSM-4-IFUP: Interface vlan172 is up

May 07 20:47:34 2012: KERN: vlan172: add 01:00:5e:00:00:01 mcast address to master interface.

May 07 20:47:34 2012: %DAEMON-3-ERR: dhcrelay: interface allocate: vlan1

May 07 20:47:34 2012: %PM-6-PROCSTART: Starting process "/usr/sbin/sshd"

May 07 20:47:34 2012: %DAEMON-3-ERR: dhcrelay: idataplane enabled

nterface allocatCCB:21:Firewall enabled

e : vlan1

May 07 20:47:34 2012: %DAEMON-3-ERR: dhcrelay: interface allocate : vlan2

May 07 20:47:34 2012: %KERN-4-WARNING: dataplane enabled.

May 07 20:47:34 2012: %DATAPLANE-5-FWSTARTUP: Firewall enabled.

May 07 20:47:39 2012: %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:May 07 18:14:32 20120: %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

May 07 20:41:28 2012: %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

In this appendix

This section describes the activities required to configure a WLAN. Instructions are provided using the wireless controller CLI.

Creating a First Controller Managed WLAN

It is assumed you have a Brocade Mobility RFS4000 wireless controller with the latest build. 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.

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.
- It is assumed the Brocade Mobility 650 Access Point also has 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.

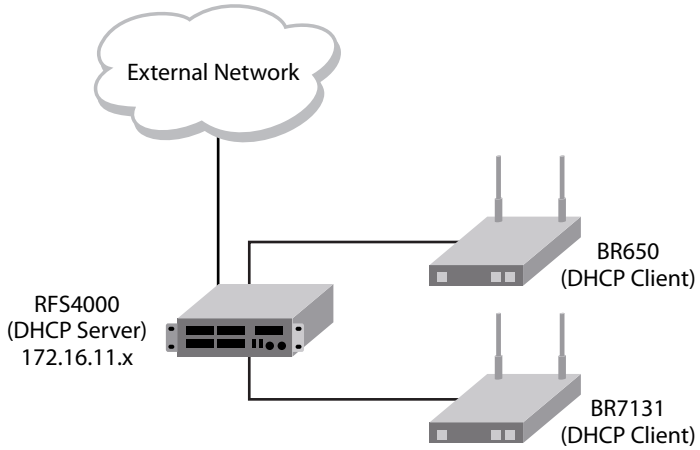


FIGURE 1 Network Design

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 VLAN2. Exit the VLAN2 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 1 to this interface. This assigns the IP address to the selected physical interface.

```
rfs4000(config-profile-RBrocade 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 1 to the GE4 interface.

```
rfs4000(config-profile-Brocade Mobility RFS4000_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 the VLAN 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 an Brocade Mobility 650 Access Point Profile*
- *Creating an Brocade Mobility 71XX Access Point Profile*

Creating an Brocade Mobility 650 Access Point Profile

Creating an AP Profile

An 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 A-1057*. In this section, the VLAN was defined as VLAN 2. Configure the access point to be a member of VLAN 2.

```
rfs4000(config-profile-BR650_UseCase1)#interface vlan 2
rfs4000(config-profile-BR650_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 BR650_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 an 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 A-1057*. 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 VLAN1 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 BR7131_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 75 displays how IP addresses are used.

TABLE 75 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-1055*. 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.

A