Ruckus Wireless™ ZoneDirector™ Command Line Interface

Reference Guide

Current as of ZoneDirector firmware version 9.6.2

Part Number 800-70497-001 Rev B
Published December 2013

www.ruckuswireless.com

Contents

About This Guide

This *Ruckus Wireless ZoneDirector Command Line Interface Reference Guide* contains the syntax and commands for configuring and managing ZoneDirector from a command line interface.

This guide is written for service operators and system administrators who are responsible for managing, configuring, and troubleshooting Ruckus Wireless devices. Consequently, it assumes a basic working knowledge of local area networks, wireless networking, and wireless devices.

NOTE: If a release note is shipped with ZoneDirector your Ruckus Wireless product and the information there differs from the information in this guide, follow the instructions in the release note.

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the Ruckus Wireless Support Web site at:

http://support.ruckuswireless.com/

Conventions

Table 1 and Table 2 list the text and notice conventions that are used throughout this guide.

Table 1. Text Conventions

Convention	Description	Example
`monospace`	Represents information as it appears on screen	`[Device name]>`
`monospace bold`	Represents information that you enter	`[Device name]>` **`set ipaddr 10.0.0.12`**
default font bold	Keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	Screen or page names	Click **Advanced Settings**. The *Advanced Settings* page appears.

Table 2. Notice Conventions

Icon	Notice Type	Description
	Information	Information that describes important features or instructions
	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device
	Warning	Information that alerts you to potential personal injury

Documentation Comments

Ruckus Wireless is interested in improving its documentation and welcomes your comments and suggestions. You can email your comments to Ruckus Wireless at:

docs@ruckuswireless.com

When contacting us, please include the following information:

- Document title
- Document part number (on the cover page)
- Page number (if appropriate)

For example:

- Ruckus Wireless ZoneDirector Command Line Interface Reference Guide
- Part number: 800-70497-001 Rev B
- Page 88

Please note that we can only respond to comments and questions about Ruckus Wireless product documentation at this email address. Questions related to technical support or sales should be directed in the first instance to your network supplier.

1

Understanding the ZoneDirector Command Line Interface

In This Chapter

Introduction

The Ruckus Wireless ZoneDirector command line interface (CLI) is a software tool that enables you to configure and manage ZoneDirector, Ruckus Wireless's wireless LAN controller.

Using the command line interface, you can issue commands from an operating system prompt, such as the Microsoft Windows command prompt or a Linux operating system terminal. Each command performs a specific action for configuring device settings or returning information about the status of a specific device feature.

Accessing the Command Line Interface

This section describes the requirements and the procedure for accessing the ZoneDirector CLI.

Requirements

To access the ZoneDirector CLI, you will need the following:

- A computer that you want to designate as administrative computer
- A network connection to ZoneDirector, or
- An RS-232 serial cable (type depends on the ZoneDirector model):
  - If you are using ZoneDirector 3000/5000, you need an RS-232 serial to Ethernet cable.
  - If you are using ZoneDirector 1100, you need a DB-9 RS-232 to RS-232 cable.
- A Telnet or SSH (secure shell) client program

Step 1: Connecting the Administrative Computer to ZoneDirector

The ZoneDirector Command Line Interface can be accessed in one of two ways:

- Using Telnet or SSH
- Using a Serial Connection

Using Telnet or SSH

1. Ensure that the administrative computer and ZoneDirector are on the same subnet or broadcast domain.
2. Continue to "Step 2: Start and Configure the Telnet/SSH Client".

Using a Serial Connection

The steps for connecting the administrative computer directly to ZoneDirector using a serial cable depend on the ZoneDirector model that you are using. Refer to the relevant section below.

- Connecting ZoneDirector 1100
- Connecting ZoneDirector 3000/5000

NOTE: Before continuing, make sure that both the administrative computer and ZoneDirector are both powered on.

Connecting ZoneDirector 1100

1. Connect one end of the RS-232 cable to the port labeled *Console* on ZoneDirector.
2. Connect the other end of the RS-232 cable to a COM port on the administrative computer.

Connecting ZoneDirector 3000/5000

1. Connect the RJ-45 end of the cable to the port labeled *Console* on ZoneDirector.
2. Connect the RS-232 end of the cable to a COM port on the administrative computer.

Step 2: Start and Configure the Telnet/SSH Client

Before starting this procedure, make sure that your Telnet/SSH client is already installed on the administrative computer.

NOTE: The following procedure uses PuTTY, a free and open source Telnet/SSH client, for accessing the ZoneDirector CLI. If you are using a different Telnet/SSH client, the procedure may be slightly different (although the connection settings should be the same). For more information on PuTTY, visit `www.putty.org`.

See the following section depending on your connection method:

- Using Telnet or SSH
- Using a Serial Connection

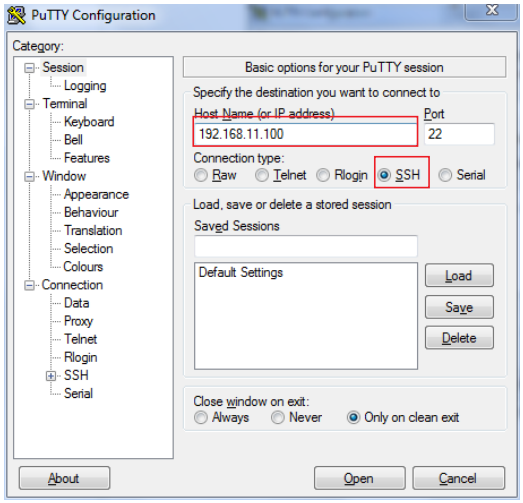
Using Telnet or SSH

To start and configure the Telnet/SSH client

1. Start PuTTY. The PuTTY Configuration dialog box appears, showing the *Session* screen.
2. In *Connection type*, select **Telnet** or **SSH**.

NOTE: Telnet access is disabled by default for security reasons. SSH is the recommended access method and you will not be allowed to access the ZoneDirector CLI via Telnet unless you have specifically enabled Telnet access. You can enable Telnet server from the ZoneDirector Web interface by going to **Configure > System > Network Management** and selecting **Enable Telnet Server**.

Figure 1. Selecting SSH as the connection type



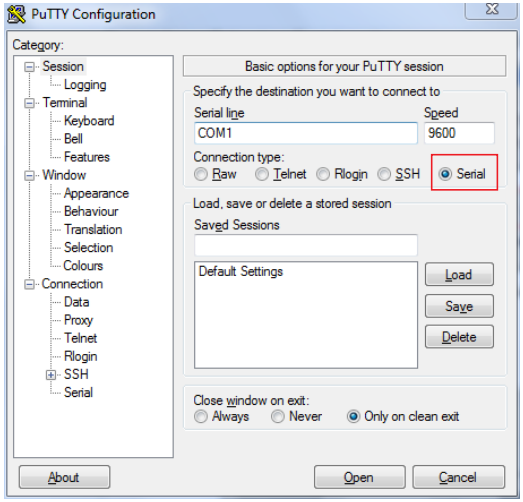
3. Enter the ZoneDirector IP address in the **Host Name (or IP address)** field.
4. Click **Open**. The PuTTY console appears and displays the login prompt.

Using a Serial Connection

To start and configure the Telnet/SSH client

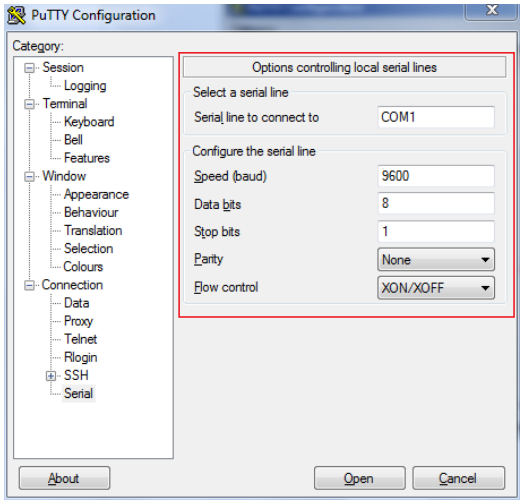
1. Start PuTTY. The PuTTY Configuration dialog box appears, showing the *Session* screen.
2. In *Connection type*, select **Serial** if you are connecting via serial cable.

Figure 2. Select Serial as the connection type



3. Under *Category*, click **Connection** > **Serial**. The serial connection options appear on the right side of the dialog box, displaying PuTTY's default serial connection settings.

Figure 3. PuTTY's default serial connection settings

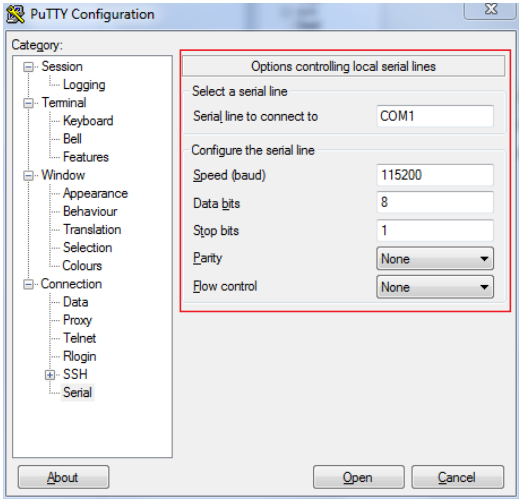


4. Configure the serial connection settings as follows:

- *Serial line to connect to*: Type the COM port name to which you connected the RS-232 cable.
- *Bits per second*: 115200
- *Data bits*: 8
- *Stop bits*: 1
- *Parity*: None

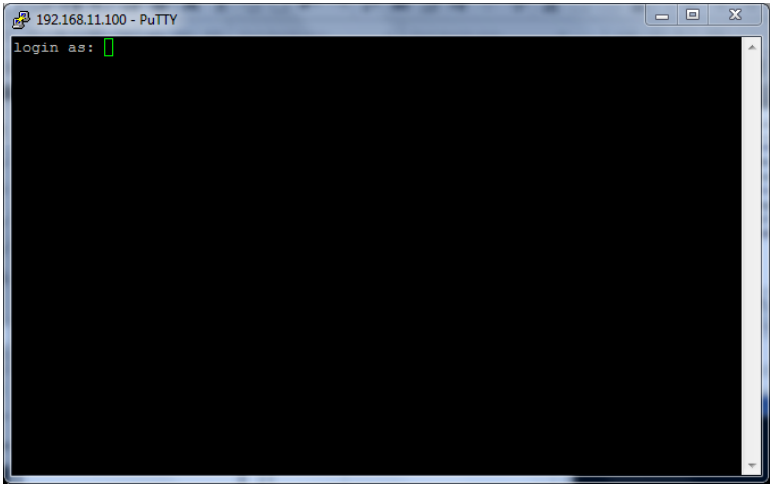
- *Flow control*: None

Figure 4. PuTTY's serial connection settings for connecting to ZoneDirector



5. Click **Open**. The PuTTY console appears and displays the login prompt.

Figure 5. The PuTTY console displaying the login prompt



You have completed configuring the Telnet/SSH client to connect to ZoneDirector.

Step 3: Log Into the CLI

1. At the login as prompt, press <Enter> once.

1. At the `Please login` prompt, type **`admin`**, and then press `<Enter>`.

2. At the `Password` prompt, type **`admin`**, and then press `<Enter>`. The Ruckus Wireless ZoneDirector CLI welcome message and the `ruckus` prompt appears.

You are now logged into the ZoneDirector CLI as a user with limited privileges. As a user with limited privileges, you can view a history of commands that were previously executed and ping a device. If you want to run more commands, you can switch to privileged mode by entering **`enable`** at the root prompt.

To view a list of commands that are available at the root level, enter **`help`** or**`?`**.

NOTE: You can tell if you are logged into the CLI in limited or privileged mode by looking at the `ruckus` prompt. If you are in limited mode, the prompt appears as `ruckus>` (with a *greater than* sign). If you are in privileged mode, the prompt appears as `ruckus#` (with a pound sign).

NOTE: To enable privileged mode when another user session is enabled, use the <force> option with the enable command to force disconnect of the previous user session. (i.e., **`enable force`**).

Using the Help Command

To display all commands that the Ruckus Wireless CLI supports, use the `help` command.

CAUTION: Entering the `help` command into the CLI prints a long list of commands on the screen. If you only want to view the commands that are available from within a specific context, use the `?` command. See "Using the ? Command" below for more information.

Using the ? Command

To display commands that are available within a specific context, use the `?` command.

Example

To display commands within the `debug` context, enter the following command:

```
ruckus# debug
ruckus(debug)# ?
```

```
  help              Shows available commands.
  history           Shows a list of previously run commands.
  quit              Exits the debug context.
  fw_upgrade        Upgrades the controller's firmware.
  delete-station    Disassociates a station.
  <MAC>
  restart-ap        Restarts a device.
  <MAC>
  wlaninfo          Configures and enables debugging of WLAN
                    service settings.
  show              Contains commands that can be executed from
                    within the context.
  ps                Displays information about all processes that
                    are running (ps -aux).
  save_debug_       Saves debug information.
  info <IP-
  ADDR>
  <FILE-NAME>
  remote_ap_c       Excutes AP CLI command in remote AP.
  li
  save-config       Upload the configuration to the designated
  <IP-ADDR>         TFTP site.
  <FILE-NAME>
  logs              Contains commands that can be executed from
                    within the context.
```

`no`	`Contains commands that can be executed from within the context.`
`remote-troubleshooting`	`Troubleshooting commands group.`
`collect_ap_coredump`	`Enable AP core dump collection.`
`script`	`Manages system script for debug.`

Top-Level Commands

The following table lists the top-level CLI commands available in privileged mode.

`exit`	End the CLI session.
`help`	Show available commands.
`quit`	End the CLI session
`history`	Show a list of previously run commands.
`disable`	Disable privileged commands.
`ping <IP-ADDR/DOMAIN-NAME>`	Send ICMP echo packets to an IP/IPv6 address or domain name.
`reboot`	Reboot the controller
`set-factory`	Reset the controller to factory defaults.
`config`	Enter the config context.
`debug`	Enter the debug context.
`show`	Display system options and settings.
`session-timeout <NUMBER>`	Set the CLI session timeout.
`monitor`	Begin system status monitoring.

2

Viewing Current Configuration

In This Chapter

Show Commands Overview

Show commands display the controller's current settings such as system status and system configuration settings, along with the status and configurations of the controller's WLAN services, users, roles, AAA servers, access points, connected clients, AP groups and WLAN groups, etc.

Monitor commands allow the administrator to enter monitoring mode to view status and configuration changes as they occur.

Show AAA Commands

Use the `show aaa` commands to display information about the authentication, authorization and accounting servers (AAA) servers that have been added to the controller.

show aaa all

To display a list of all AAA servers that have been added to the controller, use the following command:

```
show aaa all
```

Syntax Description

`show`	Display information
`aaa`	Display AAA server information
`all`	All AAA servers

Defaults

None.

Example

```
ruckus# show aaa all
AAA:
ID:
1:
Name= Local Database
Type= Local

2:
Name= Guest Accounts
Type= Guest

3:
Name= RADIUS Accounting
Type= RADIUS Accounting server
```

```
Primary RADIUS Accounting:
IP Address= 192.168.11.7
Port= 1813
Secret= secret
Secondary RADIUS Accounting:
Status= Disabled

4:
Name= Ruckus RADIUS
Type= RADIUS server
Auth Method=
Primary RADIUS:
IP Address= 192.168.11.99
Port= 1812
Secret= secret
Secondary RADIUS:
Status= Disabled

5:
Name= Ruckus AD
Type= Active Directory
IP Address= 192.168.11.17
Port= 389
Windows Domain Name= domain.ruckuswireless.com
Global Catalog= Disabled
Admin DN=domain
Admin Password=password


ruckus#
```

show aaa name

To display information about a specific AAA server that has been added to the controller, use the following command:

```
show aaa name <WORD>
```

Syntax Description

`show`	Display information
`aaa name`	Display information about the specified AAA server name
`<WORD>`	Name of the AAA server

Defaults

None.

Example

```
ruckus# show aaa name "Ruckus RADIUS"
AAA:
ID:
4:
Name= Ruckus RADIUS
Type= RADIUS server
Auth Method=
Primary RADIUS:
IP Address= 192.168.11.99
Port= 1812
Secret= secret
Secondary RADIUS:
Status= Disabled

ruckus#
```

Show DHCP Commands

Use the `show dhcp` commands to display the current settings for any DHCP servers configured for DHCP relay agent use.

show dhcp all

To display a list of all AAA servers that have been added to the controller, use the following command:

```
show dhcp all
```

Syntax Description

`show`	Display information
`dhcp`	Display information about the specified DHCP server name
`all`	Display a list of all DHCP servers

Defaults

None.

Example

```
ruckus# show dhcp all
DHCP servers for DHCP relay agent:
  ID:
    1:
```

```
      Name= DHCP Server 1
      Description=
      IP Address= 192.168.11.1
      IP Address=


ruckus#
```

show dhcp name

To display a list of all AAA servers that have been added to the controller, use the following command:

```
show dhcp name <WORD>
```

Syntax Description

`show`	Display information
`dhcp`	Display information about the specified DHCP server name
`name`	Display the DHCP server specified
`<WORD>`	Name of the DHCP server

Defaults

None.

Example

```
ruckus# show dhcp name "DHCP Server 1"
DHCP servers for DHCP relay agent:
  ID:
    1:
      Name= DHCP Server 1
      Description=
      IP Address= 192.168.11.1
      IP Address=

ruckus#
```

Show Access Point Commands

Use the `show ap` commands to display the current settings of managed devices, including their network address settings, device names, radio settings, and others.

show ap all

To display a summary of all devices that have been approved, use the following command:

```
show ap all
```

Syntax Description

`show`	Display information
`ap`	Show device information
`all`	All devices that have been approved by the controller

Defaults

None.

Example

```
ruckus# show ap all
AP:
ID:
1:
MAC Address= 04:4f:aa:0c:b1:00
Model= zf7962
Approved= Yes
Device Name= 7962 - MAP
Description= 7962 MAP (Living Room)
Location= Living Room
GPS=
Group Name= System Default
Radio a/n:
Channelization= Auto
Channel= Auto
WLAN Services enabled= Yes
5.8GHz Channels = Disabled
Tx. Power= Auto
WLAN Group Name= Default
Radio b/g/n:
Channelization= Auto
Channel= Auto
WLAN Services enabled= Yes
5.8GHz Channels = Disabled
Tx. Power= Auto
WLAN Group Name= Default
Override global ap-model port configuration= No
Network Setting:
Protocol mode= IPv4 and IPv6
```

```
Device IP Settings= Keep AP's Setting
IP Type= DHCP
IP Address= 192.168.11.6
Netmask= 255.255.255.0
Gateway= 192.168.11.1
Primary DNS Server=
Secondary DNS Server=

Device IPv6 Settings= Keep AP's Setting
IPv6 Type= Auto Configuration
IPv6 Address= fc00::1
IPv6 Prefix Length= 7
IPv6 Gateway=
IPv6 Primary DNS Server=
IPv6 Secondary DNS Server=
Mesh:
Status= Enabled
Mode= Auto
Uplink:
Status= Smart

2:
MAC Address= 00:24:82:3f:14:60
Model= zf7363
Approved= Yes
Device Name= 7363 - RAP
Description= 7363 - RAP (Study)
Location= Study
GPS=
Group Name= System Default
Radio a/n:
Channelization= Auto
Channel= Auto
WLAN Services enabled= Yes
5.8GHz Channels = Disabled
Tx. Power= Auto
WLAN Group Name= Default
Radio b/g/n:
Channelization= Auto
Channel= Auto
WLAN Services enabled= Yes
5.8GHz Channels = Disabled
```

```
Tx. Power= Auto
WLAN Group Name= Default
Override global ap-model port configuration= No
Network Setting:
Protocol mode= IPv4 and IPv6
Device IP Settings= Keep AP's Setting
IP Type= DHCP
IP Address= 192.168.11.3
Netmask= 255.255.255.0
Gateway= 192.168.11.1
Primary DNS Server= 192.168.11.1
Secondary DNS Server=

Device IPv6 Settings= Keep AP's Setting
IPv6 Type= Auto Configuration
IPv6 Address=
IPv6 Prefix Length= 7
IPv6 Gateway=
IPv6 Primary DNS Server=
IPv6 Secondary DNS Server=
Mesh:
Status= Enabled
Mode= Auto
Uplink:
Status= Smart


ruckus#
```

show ap devname

To display information about a specific device using its device name, use the following command:

```
show ap devname <WORD>
```

Syntax Description

`show`	Display information
`ap devname`	Show information about the specified device name
`<WORD>`	The name of the device

Defaults

None.

Example

```
ruckus# show ap devname "7962 - MAP"
AP:
ID:
1:
MAC Address= 04:4f:aa:0c:b1:00
Model= zf7962
Approved= Yes
Device Name= 7962 - MAP
Description= 7962 MAP (Living Room)
Location= Living Room
GPS=
Group Name= System Default
Radio a/n:
Channelization= Auto
Channel= Auto
WLAN Services enabled= Yes
5.8GHz Channels = Disabled
Tx. Power= Auto
WLAN Group Name= Default
Radio b/g/n:
Channelization= Auto
Channel= Auto
WLAN Services enabled= Yes
5.8GHz Channels = Disabled
Tx. Power= Auto
WLAN Group Name= Default
Override global ap-model port configuration= No
Network Setting:
Protocol mode= IPv4 and IPv6
Device IP Settings= Keep AP's Setting
IP Type= DHCP
IP Address= 192.168.11.6
Netmask= 255.255.255.0
Gateway= 192.168.11.1
Primary DNS Server=
Secondary DNS Server=

Device IPv6 Settings= Keep AP's Setting
IPv6 Type= Auto Configuration
IPv6 Address= fc00::1
IPv6 Prefix Length= 7
IPv6 Gateway=
```

```
IPv6 Primary DNS Server=
IPv6 Secondary DNS Server=
Mesh:
Status= Enabled
Mode= Auto
Uplink:
Status= Smart

ruckus#
```

show ap mac

To search for the device that matches the specified MAC address, use the following command:

```
show ap mac <MAC>
```

Syntax Description

`show`	Display information
`ap mac`	Display information about the device with the specified MAC address
`<MAC>`	The MAC address of the device

Defaults

None.

Example

```
ruckus# show ap mac 04:4f:aa:0c:b1:00
AP:
ID:
1:
MAC Address= 04:4f:aa:0c:b1:00
Model= zf7962
Approved= Yes
Device Name= 7962 - MAP
Description= 7962 MAP (Living Room)
Location= Living Room
GPS=
Group Name= System Default
Radio a/n:
Channelization= Auto
Channel= Auto
WLAN Services enabled= Yes
5.8GHz Channels = Disabled
```

```
Tx. Power= Auto
WLAN Group Name= Default
Radio b/g/n:
Channelization= Auto
Channel= Auto
WLAN Services enabled= Yes
5.8GHz Channels = Disabled
Tx. Power= Auto
WLAN Group Name= Default
Override global ap-model port configuration= No
Network Setting:
Protocol mode= IPv4 and IPv6
Device IP Settings= Keep AP's Setting
IP Type= DHCP
IP Address= 192.168.11.6
Netmask= 255.255.255.0
Gateway= 192.168.11.1
Primary DNS Server=
Secondary DNS Server=

Device IPv6 Settings= Keep AP's Setting
IPv6 Type= Auto Configuration
IPv6 Address= fc00::1
IPv6 Prefix Length= 7
IPv6 Gateway=
IPv6 Primary DNS Server=
IPv6 Secondary DNS Server=
Mesh:
Status= Enabled
Mode= Auto
Uplink:
Status= Smart

ruckus#
```

Show AP Group Commands

Use the show ap-group commands to display Access Point Group settings.

show ap-group all

To display all AP groups and their settings (including the default AP group), use the following command:

```
show ap-group all
```

Syntax Description

`show`	Display information
`ap-group`	Display access point group information
`all`	All AP groups

Defaults

None.

Example

```
ruckus# show ap-group all
   APGROUP:
    ID:
    1:
    Name= System Default
    Description= System default group for Access Points
    Radio 11bgn:
    Channelization= Auto
    Channel= Auto
    Enable auto channel selection which select from 1,6,11= Yes
    Tx. Power= Auto
    11N only Mode= Auto
    WLAN Group= Default
    Radio 11an:
    Channelization= Auto
    Channel= Auto
    Tx. Power= Auto
    11N only Mode= Auto
    WLAN Group= Default
    Members:
    MAC= 04:4f:aa:0c:b1:00
    MAC= 00:24:82:3f:14:60
    MAC= 74:91:1a:2b:ff:a0
```

```
APGROUP:
 ID:
 2:
 Name= ap group 2
 Description=
 Radio 11bgn:
 Channelization= Auto
 Channel= Auto
 Enable auto channel selection which select from 1,6,11= Yes
 Tx. Power= Auto
 11N only Mode= Auto
 WLAN Group= Default
 Radio 11an:
 Channelization= Auto
 Channel= Auto
 Tx. Power= Auto
 11N only Mode= Auto
 WLAN Group= Default
 Members:

APGROUP:
 ID:
 3:
 Name= ap group 1
 Description=
 Radio 11bgn:
 Channelization= Auto
 Channel= Auto
 Enable auto channel selection which select from 1,6,11= Yes
 Tx. Power= Auto
 11N only Mode= Auto
 WLAN Group= Default
 Radio 11an:
 Channelization= Auto
 Channel= Auto
```

```
 Tx. Power= Auto
 11N only Mode= Auto
 WLAN Group= Default
 Members:

ruckus#
```

show ap-group name

To display details about a specific AP group, use the following command:

```
show ap-group name <WORD>
```

Syntax Description

`show`	Display information
`ap-group name`	Display information about the AP group with the specified name
`<WORD>`	The name of the AP group

Defaults

None.

Example

```
ruckus# show ap-group name "System Default"
APGROUP:
 ID:
 1:
 Name= System Default
 Description= System default group for Access Points
 Radio 11bgn:
 Channelization= Auto
 Channel= Auto
 Enable auto channel selection which select from 1,6,11= Yes
 Tx. Power= Auto
 11N only Mode= Auto
 WLAN Group= Default
 Radio 11an:
 Channelization= Auto
 Channel= Auto
 Tx. Power= Auto
 11N only Mode= Auto
 WLAN Group= Default
 Members:
```

```
 MAC= 04:4f:aa:0c:b1:00
 MAC= 00:24:82:3f:14:60
 MAC= 74:91:1a:2b:ff:a0

ruckus#
```

Show AP Policy Commands

Use the show ap-policy command to display global access point policies that have been configured on the controller.

show ap-policy

show ap-policy

Example

```
ruckus# show ap-policy
Automatically approve all join requests from APs= Enabled
Limited ZD Discovery:
Status= Disabled
Management VLAN:
Status= Keep AP's setting
Balances the number of clients across adjacent APs= Disabled
Max. clients for 11BG radio= 100
Max. clients for 11N radio= 100
LWAPP message MTU= 1450
ruckus#
```

Show System Configuration Commands

Use the `show config` commands to display the controller's system configuration settings.

show config

To display the current system configuration settings, including network addressing, management VLAN, country code, logging, AAA servers, WLAN services, WLAN groups, AP list, SNMP, and ACLs, etc., use the following command:

```
show config
```

Syntax Description

`show`	Display information
`config`	Display system configuration settings

Defaults

None.

Example

```
ruckus# show config
Protocol Mode= IPv4-Only
Device IP Address:
Mode= Manual
IP Address= 192.168.11.100
Netmask= 255.255.255.0
Gateway Address= 192.168.11.1
Primary DNS= 192.168.11.1
Secondary DNS= 168.115.1.1

Management VLAN:
Status= Disabled
VLAN ID= 1

Country Code:
Code= United States

Identity:
Name= ruckus

NTP:
Status= Enabled
Address= ntp.ruckuswireless.com

Log:
Status= Disabled
Address=

Tunnel MTU:
Tunnel MTU= 1500

Telnet Server:
Status= Disabled

FTP Server:
Status= Enabled
```

```
Anonymous Status= Enabled

FlexMaster:
Status= Disabled
Address= flexmaster
Interval= 15

AAA:
ID:
1:
Name= Local Database
Type= Local
...
...
ruckus#
```

Show Performance Commands

Use the show performance commands to display performance details on an AP radio or client station.

show performance

Use the following command to display performance details:

```
show performance
```

show performance ap-radio2-4

Use the following command to display performance details for the AP's 2.4 GHz radio.

```
show performance ap-radio2-4 mac <MAC>
```

Syntax Description

`show performance`	Display performance information
`ap-radio-2-4`	Display AP 2.4 GHz radio performance
`mac <MAC>`	The MAC address of the AP

Defaults

None.

Example

```
ruckus# show performance ap-radio2-4 mac c4:10:8a:1f:d1:f0
AP performance:
    1:
      Radio b/g/n:
```

```
      MAC Address= c4:10:8a:1f:d1:f0
      Estimated Capacity= 9930
      Downlink= 67
      Uplink= 0
      RF pollution= 11
      Associated clients= 1
      Other APs= 0
ruckus#
```

show performance ap-radio5

Use the following command to display performance details for the AP's 5 GHz radio:

```
show performance ap-radio5 mac <MAC>
```

Syntax Description

`show performance`	Display performance information
`ap-radio-5`	Display AP 5 GHz radio performance
`mac <MAC>`	The MAC address of the AP

Defaults

None.

Example

```
ruckus# show performance ap-radio5 mac c4:10:8a:1f:d1:f0
AP performance:
    1:
      Radio a/n:
      MAC Address= c4:10:8a:1f:d1:f0
      Estimated Capacity= 20891
      Downlink= 77
      Uplink= 2
      RF pollution= 3
      Associated clients= 1
      Other APs= 0
ruckus#
```

show performance station

Use the following command to display performance details for a connected client/station:

```
show performance station mac <MAC>
```

Syntax Description

`show performance`	Display performance information
`station`	Display station performance
`mac <MAC>`	The MAC address of the station

Defaults

None.

Example

```
ruckus# show performance station mac 00:22:fb:ad:1b:2e
Station performance:
      MAC Address= 00:22:fb:ad:1b:2e
      Estimated Capacity= 61401
      Downlink= 76
      Uplink= 18
ruckus#
```

Show System Information Commands

Use the `show sysinfo` commands to display the controller's system information.

show sysinfo

To display an overview of the system status, including system, devices, usage summary, user activities, system activities, used access points, and support information, use the following command:

```
show sysinfo
```

Syntax Description

`show`	Display information
`sysinfo`	Display an overview of various system statuses

Defaults

None.

Example

```
ruckus# show sysinfo
System Overview:
Name= ruckus
IP Address= 192.168.11.100
MAC Address= 00:13:11:01:01:01
Uptime= 11d 22h 37m
Model= ZD1112
Licensed APs= 12
Serial Number= 000000000011
```

```
Version= 9.3.0.0 build 80

Devices Overview:
Number of APs= 2
Number of Client Devices= 1
Number of Rogue Devices= 0

Usage Summary:
Usage of 1 hr:
Max. Concurrent Users= 1
Bytes Transmitted= 407.13K
Number of Rogue Devices= 0
Usage of 24 hr:
Max. Concurrent Users= 2
Bytes Transmitted= 678.94M
Number of Rogue Devices= 2

Memory Utilization:
Used Bytes= 69971968
Used Percentage= 54%
Free Bytes= 59187200
Free Percentage= 46%

ruckus#
```

Show Ethernet Info Commands

Use the show ethinfo command to display current system Ethernet status.

show ethinfo

```
show ethinfo
```

Syntax Description

show	Display information
ethinfo	Display the current system Ethernet status

Defaults

None.

Example

```
ruckus# show ethinfo
System Ethernet Overview:
```

```
  Port  0:
    Interface= eth0
    MAC Address= 00:13:11:01:01:01
    Physical Link= up
    Speed= 1000Mbps
  Port  1:
    Interface= eth1
    MAC Address= 00:13:11:01:01:02
    Physical Link= up
    Speed= 100Mbps

ruckus#
```

Show Technical Support Commands

Use the following commands to display information that Ruckus Wireless may need when providing technical support.

show techsupport

To display system information required by Technical Support, use the following command:

```
show techsupport
```

Syntax Description

`show`	Display information
`techsupport`	Display information about the controller that may be required by Ruckus Wireless Technical Support

Defaults

None.

Example

```
ruckus# show techsupport
System Overview:
Name= ruckus
IP Address= 192.168.11.100
MAC Address= 00:13:11:01:01:01
Uptime= 11d 22h 46m
Model= ZD1112
Licensed APs= 12
Serial Number= 000000000011
Version= 9.3.0.0 build 80
```

```
Devices Overview:
Number of APs= 2
Number of Client Devices= 1
Number of Rogue Devices= 0

Usage Summary:
Usage of 1 hr:
Max. Concurrent Users= 1
Bytes Transmitted= 697.85K
Number of Rogue Devices= 0
Usage of 24 hr:
Max. Concurrent Users= 2
Bytes Transmitted= 679.21M
Number of Rogue Devices= 2

Memory Utilization:
Used Bytes= 70119424
Used Percentage= 54%
Free Bytes= 59039744
Free Percentage= 46%

Protocol Mode= IPv4-Only
Device IP Address:
Mode= Manual
IP Address= 192.168.11.100
Netmask= 255.255.255.0
Gateway Address= 192.168.11.1
Primary DNS= 192.168.11.1
Secondary DNS= 168.95.1.1

Management VLAN:
Status= Disabled
VLAN ID=

Country Code:
Code= United States

Identity:
Name= ruckus

NTP:
```

```
Status= Enabled
Address= ntp.ruckuswireless.com

Log:
Status= Disabled
Address=

Tunnel MTU:
Tunnel MTU= 1500

Telnet Server:
Status= Disabled

FTP Anonymous Access:
Status= Enabled

FlexMaster:
Status= Disabled
Address= flexmaster
Interval= 15

AAA:
ID:
1:
Name= Local Database
Type= Local

...
...
ruckus#
```

Show Management ACL Commands

Use the `mgmt-acl` and `mgmt-acl-ipv6` commands to display information about the management access control lists configured on the controller.

show mgmt-acl all

To display all management ACLs that have been configured on the controller, use the following command:

```
show mgmt-acl all
```

show mgmt-acl name

To display information about a specific management ACL, use the following command:

```
show mgmt-acl name <NAME>
```

show mgmt-acl-ipv6 all

To display all management ACLs that have been configured on the controller, use the following command:

```
show mgmt-acl-ipv6 all
```

show mgmt-acl-ipv6 name

To display information about a specific management ACL, use the following command:

```
show mgmt-acl-ipv6 name <NAME>
```

Syntax Description

`show`	Display information
`mgmt-acl`	Display management ACL settings
`mgmt-acl-ipv6`	Display IPv6 management ACL settings
`all`	All configured management ACLs
`name`	Display information about a specific management ACL
`<NAME>`	The name of the management ACL

Defaults

None.

Example

```
ruckus# show mgmt-acl all
Management ACL:
Name= New Name
Restriction Type= range
IP range= 192.168.11.1-192.168.11.253

Name= Remote 1
Restriction Type= single
IP address= 172.17.17.150

Name= Remote admin 2
Restriction Type= single
IP address= 172.17.16.12
```

```
ruckus#
```

Show Static Route Commands

Use the `static-route` commands to display information about static routes configured on the controller.

show static-route all

To display all static route information, use the following command:

```
show static-route all
```

show static-route name

```
show static-route name <NAME>
```

show static-route-ipv6 all

```
show static-route-ipv6 all
```

show static-route-ipv6 name

```
show static-route-ipv6 name <NAME>
```

Syntax Description

`show`	Display information
`static-route`	Display static route settings
`static-route-ipv6`	Display IPv6 static route settings
`all`	All configured static routes
`name`	Display information about a specific configured static route
`<NAME>`	The name of the static route entry

Defaults

None.

Example

```
ruckus# show static-route all
Static Route:
ID= 1
Name= Static Route 1
IP subnet= 192.168.11.1/24
IP gateway= 192.168.11.1
```

```
ruckus#
```

Show WLAN Commands

Use the following commands to display information about available WLANs on the controller.

show wlan all

To display all available WLAN services (SSIDs), use the following command:

```
show wlan all
```

Syntax Description

`show`	Display information
`wlan`	Display WLAN services (SSIDs) settings
`all`	All available WLANs/SSIDs

Defaults

None.

Example

```
ruckus# show wlan all
WLAN Service:
ID:
1:
NAME = Ruckus1
Tx. Rate of Management Frame(2.4GHz) = 2.0Mbps
Beacon Interval = 100ms
SSID = Ruckus1
Description = Ruckus WPA WLAN
Type = Standard Usage
Authentication = open
Encryption = wpa2
Algorithm = aes
Passphrase = testing123
Web Authentication = Disabled
Authentication Server = Disabled
Tunnel Mode = Disabled
Background Scanning = Enabled
Max. Clients = 100
Client Isolation = None
Zero-IT Activation = Enabled
```

```
Priority = High
Load Balancing = Enabled
Dynamic PSK = Enabled
Rate Limiting Uplink = Disabled
Rate Limiting Downlink = Disabled
Auto-Proxy configuration:
Status = Disabled
Inactivity Timeout:
Status = Enabled
Timeout = 500 Minutes
VLAN = Disabled
Dynamic VLAN = Disabled
Closed System = Disabled
ofdm-only State = Disabled
DHCP Option82 State= Disabled
BSS Minrate = Disabled
PMK Cache Time = 720 Minutes
NAS-ID Type = wlan-bssid
PAP Message Authenticator = Enabled
Send EAP-Failure = Disabled
L2/MAC = No ACLS
L3/L4/IP Address = No ACLS
L3/L4/IPv6 Address = No ACLS


ruckus#
```

show wlan name

To display information about the specified WLAN service (SSID), use the following command:

```
show wlan name <NAME>
```

Syntax Description

`show`	Display information
`wlan name`	Display information about the specified WLAN name
`<NAME>`	The name of the WLAN

Defaults

None.

Example

```
ruckus# show wlan name Ruckus1
```

```
WLAN Service:
ID:
1:
NAME = Ruckus1
Tx. Rate of Management Frame(2.4GHz) = 2.0Mbps
Beacon Interval = 100ms
SSID = Ruckus1
Description = Ruckus WPA WLAN
Type = Standard Usage
Authentication = open
Encryption = wpa2
Algorithm = aes
Passphrase = testing123
Web Authentication = Disabled
Authentication Server = Disabled
Tunnel Mode = Disabled
Background Scanning = Enabled
Max. Clients = 100
Client Isolation = None
Zero-IT Activation = Enabled
Priority = High
Load Balancing = Enabled
Dynamic PSK = Enabled
Rate Limiting Uplink = Disabled
Rate Limiting Downlink = Disabled
Auto-Proxy configuration:
Status = Disabled
Inactivity Timeout:
Status = Enabled
Timeout = 500 Minutes
VLAN = Disabled
Dynamic VLAN = Disabled
Closed System = Disabled
ofdm-only State = Disabled
DHCP Option82 State= Disabled
BSS Minrate = Disabled
PMK Cache Time = 720 Minutes
NAS-ID Type = wlan-bssid
PAP Message Authenticator = Enabled
Send EAP-Failure = Disabled
L2/MAC = No ACLS
L3/L4/IP Address = No ACLS
```

```
L3/L4/IPv6 Address = No ACLS

ruckus#
```

show wlan name stations

To display a list of wireless stations associated with the specified WLAN service, use the following command:

```
show wlan name <NAME> stations
```

Syntax Description

`show`	Display information
`wlan name`	Display information about the specified WLAN name
`<NAME>`	The name of the WLAN
`stations`	Display stations associated with the WLAN

Defaults

None.

Example

```
ruckus# show wlan name Ruckus1 stations
Clients List:
Client:
MAC Address= 6c:62:6d:1b:e3:00
User Name=
IP Address= 192.168.11.11
IPv6 Address=
Access Point= 04:4f:aa:0c:b1:00
WLAN= Ruckus1
Channel= 6
Signal (dB)= 51

Client:
MAC Address= 00:22:fb:ad:1b:2e
User Name=
IP Address= 192.168.11.7
IPv6 Address=
Access Point= 04:4f:aa:0c:b1:00
WLAN= Ruckus1
Channel= 153
Signal (dB)= 0

ruckus#
```

Show WLAN Group Commands

Use the following commands to display information about the WLAN groups that exist on the controller.

show wlan-group all

To display a list of existing WLAN groups, use the following command:

```
show wlan-group all
```

Syntax Description

`show`	Display information
`wlan-group`	Display information about the specified WLAN group
`all`	Show all WLAN groups

Defaults

None.

Example

```
ruckus# show wlan-group all
WLAN Group:
ID:
1:
Name= Default
Description= Default WLANs for Access Points
WLAN Service:
WLAN1:
NAME= Ruckus1
VLAN=
WLAN2:
NAME= Ruckus2
VLAN=

2:
Name= Guest WLAN Group
Description= 1st floor APs only
WLAN Service:
WLAN1:
NAME= Ruckus-Guest
VLAN=
```

```
ruckus#
```

show wlan-group name

To display information about the specified WLAN group name, use the following command:

```
show wlan-group name <WORD>
```

Syntax Description

`show`	Display information
`wlan-group name`	Display information about the specified WLAN group name
`<WORD>`	The name of the WLAN group

Defaults

None.

Example

```
ruckus# show wlan-group name Default
WLAN Group:
ID:
1:
Name= Default
Description= Default WLANs for Access Points
WLAN Service:
WLAN1:
NAME= Ruckus1
VLAN=
WLAN2:
NAME= Ruckus2
VLAN=

ruckus#
```

Show L2 Access Control List Commands

Use the `show l2acl` commands to display Layer 2 access control list rules that have been added to the controller.

show l2acl all

To display all Layer 2 access control list (ACL) rules that have been added to the controller and their settings, use the following command:

```
show l2acl all
```

Syntax Description

show	Display information
l2acl	Display L2 ACL information
all	All L2 ACL

Defaults

None.

Example

```
ruckus# show l2acl all
L2/MAC ACL:
ID:
1:
Name= System
Description= System
Restriction: Deny only the stations listed below
Stations:
2:
Name= blocked-sta-list
Description=
Restriction: Deny only the stations listed below
Stations:
```

show l2acl name

To display the settings of a specific L2 ACL rule that has been added to the controller, use the following command:

```
show l2acl name <WORD>
```

Syntax Description

show	Display information
l2acl	Display L2 ACL information
name	Display information about the specified L2 ACL rule name
<WORD>	Name of the L2 ACL rule

Defaults

None.

Example

```
ruckus# show l2acl name 1
L2/MAC ACL:
ID:
```

```
2:
Name= 1
Description=
Restriction: Deny only the stations listed below
Stations:
MAC Address= 00:33:22:45:34:88
```

Show L3 Access Control List Commands

Use the `show l3acl` commands to display Layer 3 access control list rules that have been added to the controller.

show l3acl all

To display all Layer 3 access control list (ACL) rules that have been added to the controller and their settings, use the following command:

```
show l3acl all
```

show l3acl-ipv6 all

To display all IPv6 Layer 3 access control list (ACL) rules that have been added to the controller and their settings, use the following command:

```
show l3acl-ipv6 all
```

Syntax Description

`show`	Display information
`l3acl`	Display L3 ACL information
`l3acl-ipv6`	Display IPv6 L3 ACL information
`all`	All L3 ACL

Defaults

None.

Example

```
ruckus# show l3acl all
L3/L4/IP ACL:
ID:
4:
Name= test2
Description= test2
Default Action if no rule is matched= Deny all by default
Rules:
Order= 1
Description=
```

```
Type= Allow
Destination Address= Any
Destination Port= 53
Protocol= Any
Order= 2
Description=
Type= Allow
Destination Address= Any
Destination Port= 67
Protocol= Any
Order= 3
Description=
Type= Allow
Destination Address= 8.8.8.8/24
Destination Port= 25
Protocol= 6
```

show l3acl name

To display the settings of a specific L3 ACL rule that has been added to the controller, use the following command:

```
show l3acl name <WORD>
```

show l3acl-ipv6 name

To display the settings of a specific IPv6 L3 ACL rule that has been added to the controller, use the following command:

```
show l3acl-ipv6 name <WORD>
```

Syntax Description

`show`	Display information
`l3acl`	Display L3 ACL information
`l3acl-ipv6`	Display IPv6 L3 ACL information
`name`	Display information about the specified L3 ACL rule
`<WORD>`	Name of the L3 ACL rule

Defaults

None.

Example

```
ruckus# show l3acl name test2
L3/L4/IP ACL:
ID:
```

```
4:
Name= test2
Description= test2
Default Action if no rule is matched= Allow all by default
Rules:
Order= 1
Description=
Type= Allow
Destination Address= Any
Destination Port= 53
Protocol= Any
Order= 2
Description=
Type= Allow
Destination Address= Any
Destination Port= 67
Protocol= Any
Order= 3
Description=
Type= Allow
Destination Address= 8.8.8.8/24
Destination Port= 25
Protocol= 6
```

Show Hotspot Commands

Use the `show hotspot` commands to display the controller's hotspot configuration settings.

show hotspot all

To display a list of all hotspot services that have been created on the controller, use the following command:

```
show hotspot all
```

Syntax Description

`show`	Display information
`hotspot`	Display hotspot information
`all`	All available hotspots

Defaults

None.

Example

```
ruckus# show hotspot all
Hotspot:
ID:
1:
Name= New Name
Login Page Url= myhotspot.com
Start Page= redirect to the URL that the user intends to visit.
Session Timeout= Disabled
Idle Timeout= Disabled
Authentication Server= Local Database
Accounting Server= Disabled
Location ID=
Location Name=
Walled Garden 1=
Walled Garden 2=
Walled Garden 3=
Walled Garden 4=
Walled Garden 5=
 IPv4 Rules:

 IPv6 Rules:

ID:
2:
Name= New name2
Login Page Url= myhotspot.com
Start Page= redirect to the URL that the user intends to visit.
Session Timeout= Disabled
Idle Timeout= Disabled
Authentication Server= Local Database
Accounting Server= Disabled
Location ID=
Location Name=
Walled Garden 1=
Walled Garden 2=
Walled Garden 3=
Walled Garden 4=
Walled Garden 5=
 IPv4 Rules:
Order= 1
Description= 10.9.5.55
Type= Deny
```

```
Destination Address= Any
Destination Port= Any
Protocol= Any

 IPv6 Rules:
```

show hotspot name

To display information about the specific hotspot service, use the following command:

```
show hotspot name <WORD>
```

If the hotspot name includes a space, you must put the name in quotation marks (for example, "hotspot name".

Syntax Description

`show`	Display information
`hotspot name`	Display hotspot information
`<WORD>`	The name of the hotspot

Defaults

None.

Example

```
ruckus# show hotspot name "New name2"
Hotspot:
ID:
2:
Name= New name2
Login Page Url= myhotspot.com
Start Page= redirect to the URL that the user intends to visit.
Session Timeout= Disabled
Idle Timeout= Disabled
Authentication Server= Local Database
Accounting Server= Disabled
Location ID=
Location Name=
Walled Garden 1=
Walled Garden 2=
Walled Garden 3=
Walled Garden 4=
Walled Garden 5=
 IPv4 Rules:
Order= 1
Description= 10.9.5.55
Type= Deny
```

```
Destination Address= Any
Destination Port= Any
Protocol= Any

 IPv6 Rules:
```

show hs20op all

To display information about all Hotspot 2.0 Operators, use the following command:

```
show hs20op all
```

Syntax Description

`show`	Display information
`hs20op`	Display Hotspot 2.0 Operator
`all`	Display all HS2.0 operators

Defaults

None.

Example

```
ruckus# show hs20op all
Hotspot 2.0 Operator:
  ID:
    1:
      NAME= operator1
      Description=
      Venue Group= Unspecified
      Venue Type= Unspecified
      ASRA Option:
        Status= Disabled
      Internet Option= Disabled
      Access Network Type= Private
      IPv4 Address Type= Not Available
      IPv6 Address Type= Not Available
      HESSID=
      Friendly Name List:
      Service Provider Profiles:
        ID= 1
          Name= provider1
      WAN Metrics:
        Enable Symmetric Link= Disabled
        WAN at Capability= Disabled
        Link Status= Link Up
        WAN Downlink Load= 0
```

```
  WAN Downlink Speed= 0
  WAN Uplink Load= 0
  WAN Uplink Speed= 0
  Load Measurement Duration= 0
Connection Capability:
  Description= ICMP
    IP Protocol= 1
    Port Number= 0
      Status= Closed
  Description= FTP
    IP Protocol= 6
    Port Number= 20
      Status= Closed
  Description= SSH
    IP Protocol= 6
    Port Number= 22
      Status= Closed
  Description= HTTP
    IP Protocol= 6
    Port Number= 80
      Status= Closed
  Description= Used by TLS VPNs
    IP Protocol= 6
    Port Number= 443
      Status= Closed
  Description= Used by PPTP VPNs
    IP Protocol= 6
    Port Number= 1723
      Status= Closed
  Description= VoIP
    IP Protocol= 6
    Port Number= 5060
      Status= Closed
  Description= Used by IKEv2 (IPSec VPN)
    IP Protocol= 17
    Port Number= 500
      Status= Closed
  Description= VoIP
    IP Protocol= 17
    Port Number= 5060
      Status= Closed
  Description= May be used by IKEv2 (IPSec VPN)
```

```
        IP Protocol= 17
        Port Number= 4500
          Status= Closed
      Description= ESP, used by IPSec VPNs
        IP Protocol= 50
        Port Number= 0
          Status= Closed
      Additional Connection Capability:
    Advanced GAS Settings:
      GAS query response buffering time= 1000
      GAS DOS detection= Disabled
      GAS DOS maximum request number= 200
    Hotspot 2.0 Capability:
      Operatiing Class Indication= Unspecified


ruckus#
```

show hs20op name

To display information about the named Hotspot 2.0 Operator, use the following command:

```
show hs20op name <WORD>
```

Syntax Description

`show`	Display information
`hs20op name`	Display specific Hotspot 2.0 Operator
`<WORD>`	The name of the HS2.0 operator

Defaults

None.

Example

```
ruckus# show hs20op name operator1
Hotspot 2.0 Operator:
  ID:
    1:
      NAME= operator1
      Description=
      Venue Group= Unspecified
      Venue Type= Unspecified
      ASRA Option:
        Status= Disabled
      Internet Option= Disabled
```

```
Access Network Type= Private
IPv4 Address Type= Not Available
IPv6 Address Type= Not Available
HESSID=
Friendly Name List:
Service Provider Profiles:
  ID= 1
    Name= provider1
WAN Metrics:
  Enable Symmetric Link= Disabled
  WAN at Capability= Disabled
  Link Status= Link Up
  WAN Downlink Load= 0
  WAN Downlink Speed= 0
  WAN Uplink Load= 0
  WAN Uplink Speed= 0
  Load Measurement Duration= 0
Connection Capability:
  Description= ICMP
    IP Protocol= 1
    Port Number= 0
      Status= Closed
  Description= FTP
    IP Protocol= 6
    Port Number= 20
      Status= Closed
  Description= SSH
    IP Protocol= 6
    Port Number= 22
      Status= Closed
  Description= HTTP
    IP Protocol= 6
    Port Number= 80
      Status= Closed
  Description= Used by TLS VPNs
    IP Protocol= 6
    Port Number= 443
      Status= Closed
  Description= Used by PPTP VPNs
    IP Protocol= 6
    Port Number= 1723
      Status= Closed
```

```
      Description= VoIP
        IP Protocol= 6
        Port Number= 5060
          Status= Closed
      Description= Used by IKEv2 (IPSec VPN)
        IP Protocol= 17
        Port Number= 500
          Status= Closed
      Description= VoIP
        IP Protocol= 17
        Port Number= 5060
          Status= Closed
      Description= May be used by IKEv2 (IPSec VPN)
        IP Protocol= 17
        Port Number= 4500
          Status= Closed
      Description= ESP, used by IPSec VPNs
        IP Protocol= 50
        Port Number= 0
          Status= Closed
      Additional Connection Capability:
    Advanced GAS Settings:
      GAS query response buffering time= 1000
      GAS DOS detection= Disabled
      GAS DOS maximum request number= 200
    Hotspot 2.0 Capability:
      Operatiing Class Indication= Unspecified

ruckus#
```

show hs20sp all

To display information about the Hotspot 2.0 Service Provider, use the following command:

```
show hs20sp all
```

Syntax Description

`show`	Display information
`hs20sp`	Display Hotspot 2.0 Service Provider
`all`	Display all HS2.0 Service Providers

Defaults

None.

Example

```
ruckus# show hs20sp all
Hotspot 2.0 Service Provider:
  ID:
    1:
      NAME= provider1
      Description=
      Realm List:
      Domain Name List:
      Roaming Consortium List:
      3GPP Cellular Network information:


ruckus#
```

show hs20sp name

To display information about a specific Hotspot 2.0 Service Provider, use the following command:

```
show hs20sp name <WORD>
```

Syntax Description

show	Display information
hs20sp name	Display specific Hotspot 2.0 Service Provider
<WORD>	The name of the HS2.0 Service Provider

Defaults

None.

Example

```
ruckus# show hs20sp name provider1
Hotspot 2.0 Service Provider:
  ID:
    1:
      NAME= provider1
      Description=
      Realm List:
      Domain Name List:
      Roaming Consortium List:
      3GPP Cellular Network information:

ruckus#
```

Show Role Commands

Use the `show role` commands to display details about roles that have been created on the controller.

show role all

To display a list of all roles that have been created on the controller, use the following command:

```
show role all
```

Syntax Description

`show`	Display information
`role`	Display role information
`all`	All roles that have been created

Defaults

None.

Example

```
ruckus# show role all
Role:
ID:
1:
Name= Default
Description= Allow Access to All WLANs
Group Attributes=
Guest Pass Generation= Allowed
ZoneDirector Administration= Disallowed
Allow All WLANs= Allow access to all WLANs.
```

show role name

To display information about the specific role, use the following command:

```
show role name <WORD>
```

Syntax Description

`show`	Display information
`role name`	Display role information
`<WORD>`	The name of the role

Defaults

None.

Example

```
ruckus# show role name Default
Role:
ID:
1:
Name= Default
Description= Allow Access to All WLANs
Group Attributes=
Guest Pass Generation= Allowed
ZoneDirector Administration= Disallowed
Allow All WLANs= Allow access to all WLANs.
```

Show User Commands

Use the `show user` commands to display details about user accounts that exist on the controller.

show user all

To display a list of all existing user accounts, use the following command:

```
show user all
```

Syntax Description

`show`	Display information
`user`	Display user information
`all`	All existing user accounts

Defaults

None.

Example

```
ruckus# show user all
User:
ID:
1:
User Name= test22
Full Name= test11
Password= test1234
Role= Default
```

show user name

To display information about the specific user, use the following command:

```
show user name <user_name>
```

Syntax Description

`show`	Display information
`user name`	Display user information
`<WORD>`	The name of the user

Defaults

None.

Example

```
ruckus# show user name test22
User:
ID:
1:
User Name= test22
Full Name= test11
Password= test1234
Role= Default
```

Show Currently Active Clients Commands

Use the `show current-active-clients` commands to display a list of wireless clients that are associated with the APs that the controller manages.

show current-active-clients all

To display a list of all existing user accounts, use the following command:

```
show current-active-clients all
```

Syntax Description

`show`	Display information
`current-active-clients`	Display currently active wireless clients
`all`	All active wireless clients

Defaults

None.

Example

```
ruckus# show current-active-clients all
Current Active Clients:
Clients:
Mac Address= 00:22:fb:5c:e2:32
User/IP= 172.18.30.2
User/IPv6=
Access Point= 04:4f:aa:13:30:f0
```

```
BSSID= 04:4f:aa:13:30:fa
Connect Since=2011/03/01 02:48:22
Auth Method= OPEN
WLAN= 11jojoe
VLAN= None
Channel= 6
Radio= 802.
Signal= 0
Status= Authorized

Last 300 Events/Activities:
Activity:
Date/Time= 2011/03/01 02:49:05
Severity= Low
User=
Activities= User[00:22:fb:5c:e2:32] joins WLAN[11jojoe] from
AP[04:4f:aa:13:30:f0]
Activity:
Date/Time= 2011/03/01 02:48:22
Severity= Low
User=
Activities= User[00:22:fb:5c:e2:32] joins WLAN[11jojoe] from
AP[04:4f:aa:13:30:f0]
...
...
ruckus#
```

show current-active-clients mac

To display information about the specific active client, use the following command:

```
show current-active-clients mac <MAC>
```

Syntax Description

`show`	Display information
`current-active-clients mac`	Display currently active wireless clients
`<MAC>`	The MAC address of the wireless client

Defaults

None.

Example

```
ruckus# show current-active-clients mac 6c:62:6d:1b:e3:00
Current Active Clients:
```

```
Clients:
Mac Address= 6c:62:6d:1b:e3:00
User/IP= 192.168.11.11
User/IPv6=
Access Point= 04:4f:aa:0c:b1:00
BSSID= 04:4f:aa:0c:b1:08
Connect Since=2012/01/10 06:22:44
Auth Method= OPEN
WLAN= Ruckus1
VLAN= None
Channel= 6
Radio= 802.11gn
Signal= 53
Status= Authorized
Received from client= 20746 pkts / 6274531 bytes
Transmitted to client= 25777 pkts / 6714433 bytes
Tx. drops due to retry failure= 1 pkts

Last 300 Events/Activities:
Activitiy:
Date/Time= 2012/01/10 06:22:44
Severity= Low
User=
Activities= User[6c:62:6d:1b:e3:00] joins WLAN[Ruckus1] from
AP[7962 - MAP@04:4f:aa:0c:b1:00]
Activitiy:
Date/Time= 2012/01/09 18:52:28
Severity= Low
User=
Activities= User[6c:62:6d:1b:e3:00] disconnects from WLAN[Ruckus1]
at AP[7363 - RAP@00:24:82:3f:14:60]
Activitiy:
Date/Time= 2012/01/08 06:08:52
Severity= Low
User=
Activities= AP[7363 - RAP@00:24:82:3f:14:60] radio [11g/n] detects
User[6c:62:6d:1b:e3:00] in WLAN[Ruckus1] roams from AP[7962 -
MAP@04:4f:aa:0c:b1:00]
...
...
ruckus#
```

Show Mesh Commands

Use the `show mesh` commands to display the controller's mesh network configuration and topology.

show mesh info

To display a list of all mesh networks that have been formed, use the following command:

```
show mesh info
```

Syntax Description

`show`	Display information
`mesh`	Display mesh network information
`info`	Show mesh information

Defaults

None.

Example

```
ruckus# show mesh info
Mesh Settings:
Mesh Status= Enabled
Mesh Name(ESSID)= Mesh-000000000311
Mesh Passphrase= GdxW5CUgrn_SEHOPyCSxv_cQHSca MH-OpnRGfX sRvwXBJL-
wUsD6eeK8CMEZfm
Mesh Hop Detection:
Status= Disabled
Mesh Downlinks Detection:
Status= Disabled
Tx. Rate of Management Frame=2Mbps
Beacon Interval= 200ms
ruckus#
```

show mesh topology

To display the topology of existing mesh networks, use the following command:

```
show mesh topology
```

Syntax Description

`show`	Display information
`mesh`	Display mesh network information
`topology`	Show mesh topology

Defaults

None.

Example

```
ruckus# show mesh topology
Mesh Topology(Mesh-000000000311):
Root Access Points= 00:24:82:3b:14:60
Signal (dB) Downlink=/ Uplink=
Description= 7363 - RAP (Study)
Channel= 153 (11an)
IP Address= 192.168.11.3
Mesh Access Points= 04:4f:ab:0c:b1:00
Signal (dB) Downlink= 28 / Uplink= 30
Description= 7962 MAP (Living Room)
Channel= 153
IP Address= 192.168.11.6

ruckus#
```

Show Dynamic PSK Commands

Use the `show dynamic-psks` commands to display information about Dynamic PSKs that have been generated. Use the following command:

```
show dynamic-psks
```

Syntax Description

`show`	Display information
`dynamic-psks`	Display dynamic PSKs that have been generated

Defaults

None.

Example

```
ruckus# show dynamic-psks
Generated Dynamic PSKs:
DPSK:
User= BatchDPSK_User_1
Mac Address= 00:00:00:00:00:00
Created= 2011/03/01 03:30:01
Expired= Unlimited
DPSK:
User= BatchDPSK_User_2
Mac Address= 00:00:00:00:00:00
Created= 2011/03/01 03:30:02
```

```
Expired= Unlimited
DPSK:
User= DPSK-User-2
Mac Address= 00:11:22:33:44:55
Created= 2011/03/01 03:30:47
Expired= Unlimited
```

Show Dynamic Certificate Commands

Use the `show dynamic-certs` commands to display information about Dynamic certificates that have been generated. Use the following command:

```
show dynamic-certs
```

Syntax Description

`show`	Display information
`dynamic-certs`	Display dynamic certificates that have been generated

Defaults

None.

Example

```
ruckus# show dynamic-certs
Generated Dynamic Certs:
```

Show Guest Pass Commands

Use the `show guest-passes` commands to display information about guest passes that have been generated. Use the following command:

```
show guest-passes
```

Syntax Description

`show`	Display information
`guest-passes`	Display guest passes that have been generated

Defaults

None.

Example

```
ruckus# show guest-passes
Generated Guest Passes:
ID:
Guest Name= John Doe
Remarks=
Expires= 2012/01/11 08:32:15
Re-auth=
```

```
Creator= ruckus
Sharable= No
Wlan= Ruckus-Guest

ruckus#
```

Show Rogue Device Commands

Use the `show rogue-devices` commands to display information about rogue devices that the controller has detected on the network. Use the following command:

```
show rogue-devices
```

Syntax Description

`show`	Display information
`rogue-devices`	Display rogues devices that have been detected on the network

Defaults

None.

Example

```
ruckus# show rogue-devices
Current Active Rogue Devices:
Rogue Devices:
Mac Address= 00:25:c4:52:1c:a1
Channel= 6
Radio= 802.11bg
Type= AP
Encryption= Open
SSID= V54-HOME001
Last Detected= 2011/03/01 02:03:43

Known/Recognized Rogue Devices:
```

Show Events and Activities Commands

Use the `show events-activities` commands to display information events and network activities that have been recorded by the controller. Use the following command:

```
show events-activities
```

Syntax Description

`show`	Display information

`events-activities`	Display a list of events and activities records by the controller

Defaults

None.

Example

```
ruckus# show events-activities
ruckus# show events-activities
Last 300 Events/Activities:
Activitiy:
Date/Time= 2012/01/10 08:33:17
Severity= Low
User=
Activities= Admin[ruckus] logs in from [192.168.11.7]
Activitiy:
Date/Time= 2012/01/10 08:32:00
Severity= Low
User=
Activities= WLAN[Ruckus-Guest] with BSSID[04:4f:aa:4c:b1:08]
configuration has been updated on radio [11g/n] of AP[7962 -
MAP@04:4f:aa:0c:b1:00]
Activitiy:
Date/Time= 2012/01/10 08:32:00
Severity= Low
User=
...
...
```

Show Alarm Commands

Use the `show alarm` commands to display alarms that have been generated by the controller. Use the following command:

```
show alarm
```

Syntax Description

`show`	Display information
`alarm`	Display a list of alarms that have been generated by the controller

Defaults

None.

Example

```
ruckus# show alarm
```

```
Last 300 Alarms:
  Alarms:
    Date/Time= 2013/03/27 15:36:59
    Name= AP Lost Contact
    Severity= High
    Activities= Lost contact with AP[7372 - MAP@c0:c5:20:3b:91:f0]
  Alarms:
    Date/Time= 2013/03/18 14:44:21
    Name= ZD warm restart
    Severity= Medium
    Activities= System warm restarted with [user reboot].
...
...
ruckus#
```

Show License Commands

Use the `show license` commands to display the controller's license information, including the model number, the maximum number of APs that it can support, and the maximum number of wireless clients that managed APs can support. Use the following command:

```
show license
```

Syntax Description

`show`	Display information
`license`	Display the controller's license information

Defaults

None.

Example

```
ruckus# show license
License:
  Model= ZD1112
  Max. AP Number= 12
  Max. Client Number= 1250
ruckus#
```

Show USB Software Commands

Use the show usb-software command to display current USB software package information.

show usb-software

```
show usb-software
```

Syntax Description

`show`	Display information
`usb-software`	Display USB software package information

Defaults

None.

Example

```
ruckus# show usb-software
Sorry, the USB Software hasn't been found.
ruckus#
```

Show Session-Timeout Commands

Use the `show session-timeout` command to display the current session timeout interval.

show session-timeout

```
show session-timeout
```

Syntax Description

`show`	Display information
`session-timeout`	Display the current session timeout interval

Defaults

None.

Example

```
ruckus# show session-timeout
Current session timeout interval is 30 minutes
ruckus#
```

Show Active Wired Client Commands

Use the `show active-wired-client` commands to display information about currently active wired clients.

show active-wired-client all

```
show active-wired-client all
```

show active-wired-client mac

```
show active-wired-client mac <MAC>
```

Syntax Description

`show`	Display information
`active-wired-client`	Display the currently active wired client information
`all`	Show all wired clients
`mac`	Show a specific client information by MAC address
`<MAC>`	The MAC address of the specific client

Defaults

None.

Example

```
ruckus# show active-wired-client all
Current Active Wired Clients:

ruckus#
```

Monitor AP MAC Commands

Use the `monitor ap mac` command to monitor details on a specific access point.

monitor ap mac

```
monitor ap mac <MAC>
```

Syntax Description

`monitor`	Begin monitoring mode
`ap mac`	Designate the access point to begin monitoring
`<MAC>`	The MAC address of the specific access point

Defaults

None.

Example

```
ruckus# monitor ap mac 04:4f:aa:0c:b1:00
------------------------------------------------------------------------
---------------
ID MAC Approved Device-Name Description
104:4f:aa:0c:b1:00 Yes7962 - MAP7962 MAP (Living
------------------------------------------------------------------------
---------------
```

```
IPv4-ADDRMASK GATEWAYPRI-DNS
192.168.11.6 255.255.255.0192.168.11.1
---------------------------------------------------------------
---------------
Radio-TypeRX-Packets(M)/RX-Bytes(G) TX-Packets(M)/TX-Bytes(G)
Retries(%)
Radio a/n 36.9/2.028.6/2.00.0
Radio-TypeRX-Packets(M)/RX-Bytes(G) TX-Packets(M)/TX-Bytes(G)
Retries(%)
Radio b/g/n 37.8/2.012.4/2.00.3
---------------------------------------------------------------
---------------
Status Mode LocationUplink-Status
EnabledAuto Living Room Smart
---------------------------------------------------------------
---------------------------------------------------------------
------------------------------
ID MAC Approved Device-Name Description
104:4f:aa:0c:b1:00 Yes7962 - MAP7962 MAP (Living
---------------------------------------------------------------
---------------
IPv4-ADDRMASK GATEWAYPRI-DNS
192.168.11.6 255.255.255.0192.168.11.1
---------------------------------------------------------------
---------------
Radio-TypeRX-Packets(M)/RX-Bytes(G) TX-Packets(M)/TX-Bytes(G)
Retries(%)
Radio a/n 36.9/2.028.6/2.00.0
Radio-TypeRX-Packets(M)/RX-Bytes(G) TX-Packets(M)/TX-Bytes(G)
Retries(%)
Radio b/g/n 37.8/2.012.4/2.00.3
---------------------------------------------------------------
---------------
Status Mode LocationUplink-Status
EnabledAuto Living Room Smart
---------------------------------------------------------------
---------------------------------------------------------------
------------------------------
ID MAC Approved Device-Name Description
104:4f:aa:0c:b1:00 Yes7962 - MAP7962 MAP (Living
---------------------------------------------------------------
---------------
IPv4-ADDRMASK GATEWAYPRI-DNS
192.168.11.6 255.255.255.0192.168.11.1
```

```
------------------------------------------------------------------
---------------
Radio-TypeRX-Packets(M)/RX-Bytes(G) TX-Packets(M)/TX-Bytes(G)
Retries(%)
Radio a/n 36.9/2.028.6/2.00.0
Radio-TypeRX-Packets(M)/RX-Bytes(G) TX-Packets(M)/TX-Bytes(G)
Retries(%)
Radio b/g/n 37.8/2.012.4/2.00.3
------------------------------------------------------------------
---------------
Status Mode LocationUplink-Status
EnabledAuto Living Room Smart
------------------------------------------------------------------
---------------



ruckus#
```

Monitor Currently Active Client Commands

Use the `monitor current-active-clients` command to monitor details on a specific client.

monitor current-active-clients

```
monitor current-active-clients mac <MAC>
```

Syntax Description

`monitor`	Begin monitoring mode
`current-active-clients mac`	Designate the currently active client to begin monitoring
`<MAC>`	The MAC address of the specific client

Defaults

None.

Example

```
ruckus# monitor current-active-clients mac 00:22:fb:ad:1b:2e
------------------------------------------------------------------
---------------
04:4f:aa:0c:b1:00 192.168.11.7 Ruckus1 None Authorized
------------------------------------------------------------------
---------------
```

```
04:4f:aa:0c:b1:0c153 11an43 OPEN
--------------------------------------------------------------------
---------------
44.3/6.743.2/17.0 36
--------------------------------------------------------------------
--------------------------------------------------------------------
------------------------------


ruckus#
```

Monitor Sysinfo Commands

Use the `monitor sysinfo` command to monitor system information.

monitor sysinfo

```
monitor sysinfo
```

Syntax Description

`monitor`	Begin monitoring mode
`sysinfo`	Display the system information

Example

```
ruckus# monitor sysinfo
--------------------------------------------------------------------
---------------
IPv4-ADDR IPv6-ADDR MAC Uptime Model MAX-APs
192.168.11.100NULL 00:13:11:01:01:01 12d 1h 29mZD111212
--------------------------------------------------------------------
---------------
Number-of-APs Number-of-ClientsNumber-of-Rogues Name
2 10ruckus
--------------------------------------------------------------------
---------------
 Usage of 1 hr|Usage of 24 hr
Max-Concurrent-Users TX-BytesRogues | Max-Concurrent-Users TX-
BytesRogues
12.33M 02297.58M 2
--------------------------------------------------------------------
---------------
Used-Bytes Used-Percentage Free-BytesFree-Percentage
71675904 55% 57483264 45%
```

```
------------------------------------------------------------------
------------------------------------------------------------------
------------------------------
IPv4-ADDR IPv6-ADDR MAC Uptime Model MAX-APs
192.168.11.100NULL 00:13:11:01:01:01 12d 1h 29mZD111212
------------------------------------------------------------------
---------------
Number-of-APs Number-of-ClientsNumber-of-Rogues Name
2 10ruckus
------------------------------------------------------------------
---------------
 Usage of 1 hr|Usage of 24 hr
Max-Concurrent-Users TX-BytesRogues | Max-Concurrent-Users TX-
BytesRogues
12.39M 02297.64M 2
------------------------------------------------------------------
---------------
Used-Bytes Used-Percentage Free-BytesFree-Percentage
71675904 55% 57483264 45%
------------------------------------------------------------------
------------------------------------------------------------------
------------------------------
```

3

Configuring Controller Settings

In This Chapter

Configuration Commands Overview

This section describes the commands that you can use to configure ZoneDirector via the `config` context.From the privileged commands context, type **`config`** to enter the configuration context. To show a list of commands available from within the config context, type help or ?.

General Config Commands

The following section describes general configuration commands can be executed from within the config context.

help

Shows available commands.

history

Shows a list of previously run commands.

abort

Exits the config context without saving changes.

end

Saves changes, and then exits the config context.

exit

Saves changes, and then exits the config context.

quit

Exits the debug context without saving changes.

Configure Context Show Commands

Use the following `show` commands to display configured settings within the config context.

show aaa

Displays a list of available AAA servers.

show dhcp

Displays a list of available DHCP servers.

show admin

Displays information about the administrator settings.

show mgmt-acl

Displays a list of all management access controls.

show mgmt-acl-ipv6

Displays a list of IPv6 management access controls.

show static-route

Displays a list of all static route entries.

show static-route-ipv6

Shows the static route for IPv6.

show ap

Displays a list of all approved devices.

show l2acl

Displays a list of L2 Access Control Lists.

show l3acl

Displays a list of L3/L4/IP ACL.

show l3acl-ipv6

Displays a list of L3/L4/IPv6 ACL.

show prece

Displays a list of Precedence Policies.

show dvcpcy

Displays a list of Device Policies.

show load-balancing

Displays information about Load balancing.

show wlan

Displays a list of all WLAN services (Names).

show wlan-group

Displays a list of existing WLAN groups.

show role

Displays a list of roles.

show user

Displays a list of users.

show hotspot

Displays a list of hotspot entries.

show ap-group

Displays all AP groups.

show ap-policy

Displays the ap policy settings.

show usb-software

Displays USB Software Package information.

Configure AAA Server Commands

This section describes the commands that you can use to configure AAA server entries on the controller. The following commands can be executed from within the `config-aaa` context. To show a list of commands available from within the aaa context, type help or ?.

aaa

To create or configure an AAA server, use the following command:

```
aaa <WORD>
```

Syntax Description

aaa	Create or edit AAA server entry
<WORD>	The name of the AAA server

Defaults

None.

Example

```
ruckus(config)# aaa ruckus-auth-02
The AAA server 'ruckus-auth-02' has been loaded. To save the AAA
server, type 'end' or 'exit'.
ruckus(config-aaa)# end
The AAA server 'ruckus-auth-02' has been updated and saved.
Your changes have been saved.
ruckus(config)#
```

no aaa

To delete an AAA server from the list of AAA servers, use the following command:

```
no aaa <WORD>
```

Syntax Description

no aaa	Delete AAA server entry
<WORD>	The name of the AAA server

Defaults

None.

Example

```
ruckus(config)# no aaa ruckus-auth-02
The AAA server 'ruckus-auth-02' has been deleted.
ruckus(config)#
```

name

To set the AAA server name, use the following command from within the config-aaa context:

```
name <WORD>
```

Syntax Description

`name`	Set the name of the AAA server
`<WORD>`	The name of the AAA server

Defaults

None.

Example

```
ruckus(config)# aaa radius2
The AAA server 'radius2' has been loaded. To save the AAA server,
type 'end' or 'exit'.
ruckus(config-aaa)# name active_directory
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-aaa)# show
AAA:
  ID:
    3:
      Name= active_directory
      Type= Active Directory
      IP Address= 192.168.7.4
      Port= 389
      Windows Domain Name=
      Global Catalog= Disabled
      Admin DN=
      Admin Password=

ruckus(config-aaa)# end
The AAA server 'active_directory' has been updated and saved.
Your changes have been saved.
ruckus(config)#
```

type

To set the AAA server type, use the following command (from within the config-aaa context):

```
type [ad|ldap|radius-auth|radius-acct]
```

Syntax Description

`type ad`	Set the AAA server type to ActiveDirectory
`type ldap`	Set the AAA server type to LDAP
`type radius-auth`	Set the AAA server type to RADIUS
`type tacplus-auth`	Set the AAA server type to TACACS+

`type radius-acct`	Set the AAA server type to RADIUS Accounting

Defaults

None.

Example

```
ruckus(config)# aaa ruckus-auth-02
The AAA server 'ruckus-auth-02' has been loaded. To save the AAA
server, type 'end' or 'exit'.
ruckus(config-aaa)# type ad
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-aaa)# end
The AAA server 'ruckus-auth-02' has been updated and saved.
Your changes have been saved.
ruckus(config)#
```

auth-method

To set the authentication method to PAP or CHAP, use the following command:

```
auth-method [pap|chap]
```

Syntax Description

`auth-method [pap|chap]`	Set the RADIUS authentication method to PAP or CHAP

Defaults

None.

Example

```
ruckus(config)# aaa radius1
The AAA server 'radius1' has been loaded. To save the AAA server,
type 'end' or 'exit'.
ruckus(config-aaa)# auth-method pap
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-aaa)# end
The AAA server 'radius1' has been updated and saved.
Your changes have been saved.
ruckus(config)#
```

ip-addr

To set the AAA server's IP address, use the following command:

```
ip-addr <IP-ADDR>
```

Syntax Description

ip-addr	Set the AAA server IP address
<IP-ADDR>	Set to this IP address

Defaults

None.

Example

```
ruckus(config)# aaa radius
The AAA server 'radius' has been loaded. To save the AAA server,
type 'end' or 'exit'.
ruckus(config-aaa)# ip-addr 192.168.0.7
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-aaa)# end
The AAA server 'radius' has been updated and saved.
Your changes have been saved.
ruckus(config)#
```

ip-addr port

To set the AAA server's IP address and port number, use the following command:

```
ip-addr <IP-ADDR> port <PORT-NUM>
```

Syntax Description

ip-addr	Set the AAA server IP address
<IP-ADDR>	Set to this IP address
port	Set the AAA server's port number
<PORT-NUM>	Set the AAA server's port number to this port

Defaults

None.

Example

```
ruckus(config)# aaa radius
The AAA server 'radius' has been loaded. To save the AAA server,
type 'end' or 'exit'.
ruckus(config-aaa)# ip-addr 192.168.0.7 port 1812
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-aaa)# end
The AAA server 'radius' has been updated and saved.
Your changes have been saved.
ruckus(config)#
```

tacplus-service

To set the TACACS+ service name, use the following command:

```
tacplus-service <WORD>
```

Syntax Description

`tacplus-service`	Configure the TACPLUS service name with length (1-64 bytes).
`<WORD>`	Name of the TACPLUS service.

Example

```
ruckus(config)# aaa tacplus1
The AAA server 'tacplus1' has been created. To save the AAA server, type 'end' or 'exit'.
ruckus(config-aaa)# type tacplus-auth
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-aaa)# ip-addr 192.168.4.6
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-aaa)# tacplus-service tacplus-service-1
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-aaa)# tacplus-secret mysecret
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-aaa)# end
The AAA server 'tacplus1' has been updated and saved.
Your changes have been saved.
ruckus(config)#
```

domain-name

To set the Windows/Base domain name, use the following command:

```
domain-name <WORD>
```

Syntax Description

`domain-name`	Configure the Windows/Base domain name
`<WORD>`	Set the Windows/Base domain name to this domain name

Defaults

None.

Example

```
ruckus(config-aaa)# domain-name company.com
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

no ad-global-catalog

To disable Global Catalog support, use the following command:

```
no ad-global-catalog
```

Syntax Description

`no ad-global-catalog`	Disable Global Catalog support

Defaults

None.

Example

```
ruckus(config-aaa)# no ad-global-catalog
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

ad-global-catalog

To enable Global Catalog support, use the following command:

```
ad-global-catalog
```

Syntax Description

`ad-global-catalog`	Enable Global Catalog support

Defaults

None.

Example

```
ruckus(config-aaa)# ad-global-catalog
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

admin-dn

To set the admin domain name, use the following command:

```
admin-dn <WORD>
```

Syntax Description

`admin-dn`	Set the admin domain name

<WORD>	Set to this domain name

Defaults

None.

Example

```
ruckus(config-aaa)# admin-dn domain_of_admin
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

admin-password

To set the admin password, use the following command:

```
admin-password <WORD>
```

Syntax Description

admin-password	Set the admin password
<WORD>	Set to this password

Defaults

None.

Example

```
ruckus(config-aaa)# admin-password test1234
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

key-attribute

To set the LDAP key attribute, use the following command:

```
key-attribute <WORD>
```

Syntax Description

key-attribute	Set the LDAP key attribute
<WORD>	Set to this attribute

Defaults

None.

Example

```
ruckus(config-aaa)# key-attribute mycompany
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

search-filter

To set the LDAP search filter, use the following command:

```
search-filter <WORD>
```

Syntax Description

`search-filter`	Set the LDAP search filter
`<WORD>`	Set to this filter

Defaults

None.

Example

```
ruckus(config-aaa)# search-filter stringofsearch
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

radius-secret

To set the AAA server's shared secret, use the following command:

```
radius-secret <WORD>
```

Syntax Description

`radius-secret`	RADIUS server secret
`<WORD>`	Set the RADIUS server secret to this secret

Defaults

None.

Example

```
ruckus(config-aaa)# radius-secret mysecret
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

tacplus-secret

To set the TACPLUS server's shared secret, use the following command:

```
tacplus-secret <WORD>
```

Syntax Description

`tacplus-secret`	TACPLUS server secret
`<WORD>`	Set the TACPLUS server secret to this secret

Example

```
ruckus(config)# aaa tacplus1
The AAA server 'tacplus1' has been created. To save the AAA server,
type 'end' or 'exit'.
ruckus(config-aaa)# ip-addr 192.168.4.7
```

```
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-aaa)# type tacplus-auth
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-aaa)# tacplus-service service1
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-aaa)# tacplus-secret mysecret
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-aaa)# show
AAA:
  ID:
    :
      Name= tacplus1
      Type= TACPLUS Auth
      TACPLUS AUTH:
        IP Address= 192.168.4.7
        Port= 49
        TACPLUS SERVICE = service1
        Secret= ********

ruckus(config-aaa)# end
The AAA server 'tacplus1' has been updated and saved.
Your changes have been saved.
ruckus(config)#
```

Backup RADIUS server AAA Commands

The following commands are used to enable and configure a backup (secondary) RADIUS server.

backup

To enable a backup RADIUS server, use the following command:

```
backup
```

Syntax Description

backup	Enables secondary RADIUS server

Example

```
ruckus(config)# aaa radius
```

```
The AAA server 'radius' has been loaded. To save the AAA server,
type 'end' or 'exit'.
ruckus(config-aaa)# backup
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-aaa)# show
AAA:
ID:
6:
Name= radius
Type= RADIUS server
Auth Method= pap
Primary RADIUS:
IP Address= 192.168.0.7
Port= 1812
Secret= secret
Secondary RADIUS:
Status= Enabled
IP Address= 192.168.0.8
Port= 1812
Secret= secret
Failover Policy:
Request Timeout= 10 Seconds
Max. Number of Retries= 2 Times
Reconnect Primary= 500 Minutes
ruckus(config-aaa)# end
The AAA server 'radius' has been updated and saved.
Your changes have been saved.
ruckus(config)#
```

backup-ip-addr

To set the IP address of the secondary RADIUS server, enter the following command:

```
backup-ip-addr <IP-ADDR>
```

Syntax Description

backup-ip-addr	Sets the IP address of the secondary RADIUS server
<IP-ADDR>	Set to this IP address

Example

```
ruckus(config)# aaa radius
```

```
The AAA server 'radius' has been loaded. To save the AAA server,
type 'end' or 'exit'.
ruckus(config-aaa)# backup-ip-addr 192.168.0.8
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-aaa)# end
The AAA server 'radius' has been updated and saved.
Your changes have been saved.
ruckus(config)#
```

backup-radius-secret

To set the shared secret of the secondary RADIUS server, enter the following command:

```
backup-radius-secret <WORD>
```

Syntax Description

`backup-radius-secret`	Sets the secret of the secondary RADIUS server
`<WORD>`	Set to this secret

Defaults

None.

Example

```
ruckus(config)# aaa radius
The AAA server 'radius' has been loaded. To save the AAA server,
type 'end' or 'exit'.
ruckus(config-aaa)# backup
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-aaa)# backup-radius-secret secret
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-aaa)# end
The AAA server 'radius' has been updated and saved.
Your changes have been saved.
ruckus(config)#
```

no backup

To disable the backup RADIUS server, use the following command:

```
no backup
```

Syntax Description

`no backup`	Disable backup RADIUS server

Defaults

None.

Example

```
ruckus(config-aaa)# no backup
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

request-timeout

To set the failover request timeout (2~20 seconds), use the following command:

```
request-timeout <NUMBER>
```

Syntax Description

`request-timeout`	Set failover request timeout
`<NUMBER>`	Number of seconds (2~20 seconds) for failover request timeout

Defaults

None.

Example

```
ruckus(config-aaa)# request-timeout 10
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

retry-count

To set the failover retry count (2~10 times), use the following command:

```
retry-count <NUMBER>
```

Syntax Description

`retry-count`	Set failover retry count
`<NUMBER>`	Number of attempts (2~10 times) for failover retry count

Defaults

None.

Example

```
ruckus(config-aaa)# retry-count 5
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

reconnect-primary-interval

To set the failover reconnect to primary interval (1~86400 minutes), use the following command:

```
reconnect-primary-interval <NUMBER>
```

Syntax Description

`reconnect-primary-interval`	Set interval for reconnecting to primary AAA server after failover
`<NUMBER>`	Number of minutes (1~86400 minutes) after which reconnect to primary is attempted

Defaults

None.

Example

```
ruckus(config-aaa)# reconnect-primary-interval 600
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-aaa)#
```

Configure DHCP Server Commands

This section describes the commands that you can use to configure DHCP server entries on the controller. These DHCP server entries are used by the DHCP Relay feature, if enabled for a tunneled WLAN. The following commands can be executed from within the `config-dhcp` context.

dhcp

Use the `dhcp` command from within the config context to create or edit a DHCP server entry.

```
dhcp <WORD>
```

Syntax Description

`dhcp`	Configure the DHCP server settings
`<WORD>`	Name of the DHCP server entry

Defaults

none

Example

```
ruckus(config)# dhcp dhcp_server_2
```

```
The DHCP server 'dhcp_server_2' has been created. To save the DHCP
server, type 'end' or 'exit'.
ruckus(config-dhcp)# first 192.168.11.99
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-dhcp)# show
DHCP servers for DHCP relay agent:
  ID:
    :
      Name= dhcp_server_2
      Description=
      IP Address= 192.168.11.99

ruckus(config-dhcp)# end
The DHCP server 'dhcp_server_2' has been updated and saved.
Your changes have been saved.
ruckus(config)# show dhcp
DHCP servers for DHCP relay agent:
  ID:
    1:
      Name= DHCP Server 1
      Description=
      IP Address= 192.168.11.1
      IP Address=

    2:
      Name= dhcp_server_2
      Description=
      IP Address= 192.168.11.99
      IP Address=


ruckus(config)#
```

no dhcp

Use the no dhcp command to delete a DHCP server entry.

```
no dhcp <WORD>
```

Example

```
ruckus(config)# no dhcp dhcp_server_2
The DHCP server 'dhcp_server_2' has been deleted.
ruckus(config)#
```

show

Displays a list of available DHCP servers.

```
show
```

name

Sets the DHCP server name.

```
name <WORD>
```

description

Sets the DHCP server description.

```
description <WORD>
```

first

Sets the DHCP server's first IP address.

```
first <IP-ADDR>
```

second

Sets the DHCP server's second IP address.

```
second <IP-ADDR>
```

no second

Deletes the DHCP server's second IP address.

```
no second <IP-ADDR>
```

Configure Admin Commands

Use the `admin` commands to enter the config-admin context to set the admin user name, password and admin authentication server settings.

admin

To enter the config-admin context and configure administrator preference, use the following command:

```
admin
```

Example

```
ruckus(config)# admin
ruckus(config-admin)
```

name

To set the administrator user name, use the following command:

```
name <WORD>
```

Syntax Description

name	Configure the admin name setting
<WORD>	Set the admin name to this name

Defaults

admin

Example

```
ruckus(config)# admin
ruckus(config-admin)# name admin
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-admin)# end
The administrator preferences have been updated.
Your changes have been saved.
ruckus(config)#
```

name password

To set the admin name and password at the same time, use the following command:

```
name <WORD> password <WORD>
```

Syntax Description

name	Configure the admin name setting
<WORD>	Set the admin name to this name
password	Configure the admin password
<WORD>	Set the admin password to this password

Defaults

admin

Example

```
ruckus(config)# admin
ruckus(config-admin)# name admin password admin
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-admin)# end
The administrator preferences have been updated.
Your changes have been saved.
```

```
ruckus(config)#
```

Admin Authentication Commands

Use the `auth-server` commands to set the administrator authentication options with an external authentication server.

auth-server

To enable administrator authentication with a remote server and set the authentication server, use the following command:

```
auth-server <WORD>
```

Syntax Description

`auth-server`	Admin authentication with an external server
`<WORD>`	Set the authentication server to this server

Defaults

None.

Example

```
ruckus(config-admin)# auth-server radius
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-admin)#
```

no auth-server

To disable administrator authentication with a remote server, use the following command:

```
no auth-server
```

Syntax Description

`no auth-server`	Disable admin authentication with an external server

Defaults

None.

Example

```
ruckus(config-admin)# no auth-server
The command was executed successfully.
```

auth-server with-fallback

To enable fallback authentication (for use when the remote server is unavailable), use the following command:

```
auth-server <WORD> with-fallback
```

Syntax Description

`auth-server`	Admin authentication with an external server
`<WORD>`	Set the auth-server to this server
`with-fallback`	Enable fallback authentication if the remote authentication server is unavailable

Defaults

None.

Example

```
ruckus(config-admin)# auth-server radius with-fallback
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-admin)# show
Administrator Name/Password:
Name= admin
Password= admin
Authenticate:
Mode= Authenticate with authentication server 'radius'
Fallback= Enabled

ruckus(config-admin)#
```

Configure Access Points

The following commands can be used from within the `config-ap` context to configure a specific Access Point.

ap

To enter the `config-ap` context, enter the following command:

```
ap <MAC>
```

Syntax Description

`ap`	Access Point
`<MAC>`	MAC address of the access point for configuration

Defaults

None.

Example

```
ruckus(config)# ap 04:4f:aa:0c:b1:00
The AP '04:4f:aa:0c:b1:00' has been loaded. To save the AP, type
'end' or 'exit' .
ruckus(config-ap)#
```

no ap

To delete an AP from the list of approved devices, use the following command:

```
no ap <MAC>
```

Syntax Description

no ap	Delete Access Point
<MAC>	MAC address of the access point

Defaults

None.

Example

```
ruckus(config)# no ap 04:4f:aa:0c:b1:00
The AP '04:4f:aa:0c:b1:00' has been deleted.
ruckus(config)#
```

devname

To set the device name, use the following command:

```
devname <WORD>
```

Syntax Description

devname	Device name
<WORD>	Set the device name to this name

Defaults

None.

Example

```
ruckus(config)# ap 04:4f:aa:0c:b1:00
The AP '04:4f:aa:0c:b1:00' has been loaded. To save the AP, type
'end' or 'exit'.
ruckus(config-ap)# devname 7962
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-ap)# end
The device information has been updated.
Your changes have been saved.
```

```
ruckus(config)#
```

no devname

To delete the device's name, use the following command:

```
no devname
```

description

To set the device description, use the following command:

```
description <WORD>
```

Syntax Description

`description`	Device description
`<WORD>`	Set the device description to this text

Defaults

None.

Example

```
ruckus(config-ap-00:13:92:00:33:1C)# description this-is-the-device-description
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-ap)#
```

no description

To delete the device's description, use the following command:

```
no description
```

gps

To set the device GPS coordinates, use the following command:

```
gps <GPS-COORDINATE>
```

Syntax Description

`gps`	Set the device GPS coordinates
`<GPS-COORDINATE>`	Enter the device's GPS coordinates for the latitude and longitude. Use a comma (,) to separate the latitude and longitude. The first coordinate is for the latitude. The second coordinate is for the longitude. Ex. A,B or -37,38.

Defaults

None.

Example

```
ruckus(config-ap)# gps 37.3,-122
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-ap)#
```

no gps

To delete the device's GPS coordinates, use the following command:

```
no gps
```

location

To set the device location, use the following command:

```
location <WORD>
```

Syntax Description

`location`	Device location
`<WORD>`	Set the device location to this address

Defaults

None.

Example

```
ruckus(config-ap)# location sunnyvale-office
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-ap)#
```

no location

To delete the device's location, use the following command:

```
no location
```

group

To set the AP group for this AP, use the following command:

```
group [name <WORD>]|system-default
```

Syntax Description

`group`	Set the AP group that this AP is a member of
`name`	Set the AP to be a member of the named AP group
`<WORD>`	The name of the AP group
`system-default`	Set the AP as a member of the system default AP group

Defaults

system-default

Example

```
ruckus(config-ap)# group system-default
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-ap)#
```

ip

To set the AP's IPv4 address, use the following command from within the config-ap context:

```
ip [enable|disable] addr <IP-ADDR> <NET-MASK> name-server <DNS-
ADDR> mode [dhcp|static|keep]
```

Syntax Description

`ip`	Set the AP's IPv4 addressing
`enable`	Enable IPv4 addressing
`disable`	Disable IPv4 addressing
`addr`	Set the AP's IPv4 address
`<IP-ADDR>`	The IPv4 address
`<NET-MASK>`	The IPv4 netmask
`name-server`	Set the device's DNS servers. Use a space ( ) to separate primary and secondary DNS servers
`<DNS-ADDR>`	The IP address of the DNS server
`mode`	Set the device's IP addressing mode (DHCP, static or "keep AP's setting")
`dhcp`	Set the device's IP address mode to DHCP
`static`	Set the device's IP address mode to static
`keep`	Set the device to use its current network settings

Defaults

none

Example

```
ruckus(config-ap)# ip enable mode dhcp
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-ap)#
```

ipv6

To set the AP's IPv6 address, use the following command from within the config-ap context:

```
ipv6 [enable] addr <IPv6-ADDR> <IPv6-PREFIX-LENGTH> name-server
<DNS-ADDR> mode [auto|manual|keep]
```

Syntax Description

`ipv6`	Set the AP's IPv6 addressing
`enable`	Enable IPv6 addressing
`addr`	Set the AP's IPv6 address
`<IPv6-ADDR>`	The IPv6 address
`<IPv6-PREFIX-LENGTH>`	The IPv6 prefix length. Use a space ( ) to separate the IPv6 address and prefix length
`name-server`	Set the device's DNS servers. Use a space ( ) to separate primary and secondary DNS servers
`<DNS-ADDR>[<DNS-ADDR>]`	The IP address of the DNS server
`mode`	Set the device's IP addressing mode (auto, manual or "keep AP's setting")
`auto`	Set the device's IPv6 address mode to auto
`manual`	Set the device's IPv6 address mode to manual
`keep`	Set the device to use its current network settings

Defaults

none

Example

```
ruckus(config-ap)# ipv6 enable mode auto
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-ap)#
```

no ipv6

To disable the AP's IPv6 mode, use the following command:

```
no ipv6
```

Radio 2.4/5 GHz Commands

Use the `radio 2.4` or `radio 5` commands to configure the 2.4/5 GHz radio settings independently.

radio

Use the radio command from within the config-ap context to configure the 2.4GHz or 5GHz radios independently.

```
radio [2.4|5] <arguments>
```

Syntax Description

`2.4`	Configure the 2.4 GHz radio
`5`	Configure the 5 GHz radio
`channelization [auto|<NUMBER>]`	Set channel width to 20 MHz, 40 MHz or Auto
`channel [auto|<NUMBER>]`	Set channel to Auto or manually set channel
`tx-power [auto|full|min|num <1-10>]`	Set transmit power to auto, full, min, or a number (-1dB~-10dB)
`admission-control <VALUE>`	Set the radio to use the specified call admission control airtime usage limit (%)
`channel-range <NUMBER-LIST>`	Set the allowed list of channels for the specified radio.
`wlan-group <WORD>`	Set the AP radio as a member of a WLAN group
`wlan-service`	Enable WLAN service on this radio
`extant-gain <NUMBER>`	Set external antenna gain (on APs that support external antennas) (dBi)

Defaults

channelization: Auto

channel: Auto

wlan-group: Default

wlan-service: Enable

tx-power: Auto

Example

```
ruckus(config-ap)# radio 2.4 channelization auto
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-ap)# radio 2.4 channel auto
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-ap)# radio 2.4 wlan-group Default
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-ap)# radio 2.4 wlan-service
```

```
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-ap)# radio 2.4 tx-power auto
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-ap)# end
The device information has been updated.
Your changes have been saved.
ruckus(config)#
```

no radio

Use the `no radio 2.4` or `no radio 5` command from within the config-ap context to disable AP group overrides for the 2.4GHz or 5GHz radio settings.

```
no radio [2.4|5] <arguments>
```

Syntax Description

no radio	Disable override of 2.4/5GHz radio settings
2.4	Disable 2.4GHz radio override settings
5	Disable 5GHz radio override settings
wlan-service	Disable override of WLAN service settings.
channel-range-override	Disables override of channel range settings.
channel-override	Disables override of channel settings.
channelization-override	Disables override of 5GHz channelization settings.
tx-power-override	Disables override of Tx power.
wlan-group-override	Disables override of WLAN group settings
admission-control	Disables call admission control on the radio
admission-control-override	Disables override of call admission control settings
wlan-service	Disables override of WLAN service settings
channel-range-override	Disables override of channel range settings

Example

```
ruckus(config-ap)# no radio 2.4 tx-power-override
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-ap)#
```

mesh mode

Use the `mesh mode` command from within the config-ap context to configure the AP's mesh mode settings.

```
mesh mode [auto|root-ap|mesh-ap|disable]
```

Syntax Description

`mesh mode`	Configure the AP's mesh mode
`auto`	Set mesh mode to Auto
`root-ap`	Configure AP as a Root AP
`mesh-ap`	Configure AP as a Mesh AP
`disable`	Disable mesh

Defaults

Auto.

Example

```
ruckus(config-ap)# mesh mode auto
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-ap)#
```

mesh uplink-selection

Use the `mesh uplink-selection` command from within the config-ap context to configure the AP's mesh uplink selection settings.

```
mesh uplink-selection [auto|manual] <add-mac>|<del-mac> <MAC>
```

Syntax Description

`mesh uplink-selection`	Configure the AP's mesh uplink selection mode
`auto`	Set mesh uplink selection to Auto
`manual`	Set mesh uplink selection to manual
`add-mac`	Add a manual uplink selection AP
`del-mac`	Delete a manual uplink selection AP
`<MAC>`	The MAC address of the uplink AP

Defaults

Auto.

Example

```
ruckus(config-ap)# mesh uplink-selection manual add-mac
00:24:82:3f:14:60
```

```
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-ap)#
```

Example

```
ruckus(config-ap)# mesh uplink-selection auto
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-ap)#
```

status-leds

To enable or disable the AP's status LEDs, use the following command:

```
status-leds [enable|disable]
```

Defaults

Enabled.

Syntax Description

`status-leds`	Configure status LEDs
`enable`	Override group config, enable status LEDs
`disable`	Override group config, disable status LEDs

Example

```
ruckus(config-ap)# status-leds disable
ruckus(config-ap)#
```

no status-leds-override

To disable override of status LEDs for this AP, use the following command:

```
no status-leds-override
```

poe-out

To enable or disable the AP's PoE Out port, use the following command:

```
poe-out [enable|disable]
```

Defaults

Disabled.

Syntax Description

`poe-out`	Configure PoE Out port
`enable`	Override group config, enable PoE Out port
`disable`	Override group config, disable PoE Out port

Example

```
ruckus(config-ap)# poe-out enable
ruckus(config-ap)#
```

no poe-out-override

To disable override of the PoE out port settings, use the following command:

```
no poe-out-override
```

no usb-software override

To disable the override of the AP USB software package, use the following command:

```
no usb-software override
```

external-antenna

To configure the AP's external antenna settings, use the following command:

```
external-antenna [2.4GHz(11BG)|5GHz(11NA)] [enable|disable]
[gain <MAC>] [2-antennas|3-antennas]
```

Syntax Description

`2.4GHz(11BG)`	Configure external 2.4GHz antenna
`5GHz(11NA)`	Configure external 5GHz antenna
`enable|disable`	Enable/disable external antenna
`gain`	Set external antenna gain for 2.4/5GHz radio
`2-antennas`	Select two external antennas for the specified radio
`3-antennas`	Select three external antennas for the specified radio

no external-antenna-override

To disable override of the external antenna, use the following command:

```
no external-antenna-override
```

internal-heater

To enable or disable the AP's internal heater, use the following command:

```
internal-heater [enable|disable]
```

Defaults

Disabled.

Syntax Description

`internal-heater`	Configure internal heater
`enable`	Override group config, enable internal heater
`disable`	Override group config, disable internal heater

Example

```
ruckus(config-ap)# internal-heater enable
ruckus(config-ap)#
```

no internal-heater-override

To disable override of the internal heater for this AP, use the following command:

```
no internal-heater-override
```

cband-channels

To enable or disable the 5.8 GHz C-band channels, use the following command:

```
cband-channels [enable|disable]
```

Defaults

Disabled.

Syntax Description

`cband-channels`	Configure C-band channels
`enable`	Override group config, enable C-band channels
`disable`	Override group config, disable C-band channels

Example

```
ruckus(config-ap)# cband-channels enable
ruckus(config-ap)#
```

no cband-channels-override

To disable override of the 5.8 GHz channels, use the following command:

```
no cband-channels-override
```

usb-software

To set the AP USB software package vendor ID (VID) and product ID (PID), use the following command:

```
usb-software <VID-PID>
```

no usb-software

To delete a USB software package from the list of USB software packages, use the following command:

```
no usb-software
```

ipmode

To set the AP's IP mode, use the following command:

```
ipmode <WORD>
```

Defaults

Dual-stack IPv4/IPv6 mode

Syntax Description

`ipmode`	Configure IP addressing mode
`ipv4`	Set to IPv4 only mode
`ipv6`	Set to IPv6 only mode
`dual`	Set to dual-stack IPv4/IPv6 mode

Example

```
ruckus(config-ap)# ipmode dual
ruckus(config-ap)#
```

no ipmode-override

To disable the override of the IP mode, use the following command:

```
no ipmode-override
```

radio-band

To set the radio band of the AP, use the following command:

```
radio-band <WORD>
```

This command is available only on APs that support band switching between 2.4GHz and 5GHz radio band modes.

Syntax Description

`radio-band`	Configure radio band mode
`<WORD>`	Set to 2.4 or 5 GHz radio mode

Example

```
ruckus(config-ap)# radio-band 5
Your changes have been saved.
ruckus(config-ap)#
```

no radio-band-override

To disable AP radio band override settings, use the following command:

```
no radio-band-override
```

venue-name

To set the venue name of the AP, use the following command:

```
venue-name [language] <WORD>
```

Syntax Description

`venue-name`	Set the venue name for the AP
`[language]`	Set the language of the venue name. Valid languages are: English, Chinese, Czech, Danish, Dutch, French, German, Japanese, Spanish, Swedish, Turkish)
`<WORD>`	Set the venue name to the name specified

Example

```
ruckus(config-ap)# venue-name english venue1
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-ap)#
```

no venue-name

To remove a venue name entry, use the following command:

```
no venue-name [language]
```

Example

```
ruckus(config-ap)# no venue-name english
The entry 'English' has been removed. To save the changes, type
'end' or 'exit'.
ruckus(config-ap)#
```

show

To display the AP's current configuration settings, use the following command:

```
show
```

Example

```
ruckus(config)# ap 04:4f:aa:0c:b1:00
The AP '04:4f:aa:0c:b1:00' has been loaded. To save the AP, type
'end' or 'exit'.
ruckus(config-ap)# show
AP:
```

```
ID:
  2:
    MAC Address= 04:4f:aa:0c:b1:00
    Model= zf7962
    Approved= Yes
    Device Name= 7962 - Mesh
    Description=
    Location=
    GPS=
    CERT = Normal
    Group Name= System Default
    Channel Range:
      A/N=
36,40,44,48,52,56,60,64,100,104,108,112,116,120,124,128,132,136,1
49,153,157,161 (Disallowed= )
      B/G/N= 1,2,3,4,5,6,7,8,9,10,11,12,13 (Disallowed= )
    Radio a/n:
      Channelization= Auto
      Channel= Auto
      WLAN Services enabled= Yes
      Tx. Power= Auto
      WLAN Group Name= Default
      Call Admission Control= OFF
    Radio b/g/n:
      Channelization= Auto
      Channel= Auto
      WLAN Services enabled= Yes
      Tx. Power= Auto
      WLAN Group Name= Default
      Call Admission Control= OFF
    Override global ap-model port configuration= No
    Network Setting:
      Protocol mode= Use Parent Setting
      Device IP Settings= Keep AP's Setting
      IP Type= DHCP
      IP Address= 192.168.11.60
      Netmask= 255.255.255.0
      Gateway= 192.168.11.1
      Primary DNS Server=
      Secondary DNS Server=
```

```
        Device IPv6 Settings= Keep AP's Setting
        IPv6 Type= Auto Configuration
        IPv6 Address= fc00::1
        IPv6 Prefix Length= 7
        IPv6 Gateway=
        IPv6 Primary DNS Server=
        IPv6 Secondary DNS Server=
      Mesh:
        Status= Enabled
        Mode= Auto
      Uplink:
        Status= Smart
      Venue Name List:

ruckus(config-ap)#
```

AP Port Setting Commands

To override AP group configuration settings and configure the AP's Ethernet ports individually, you must first enter the `config-ap-model` context from within the config-ap context.

port-setting

Use the following command to enter the config-ap-model context and override AP group settings to configure AP ports individually:

```
port-setting
```

Defaults

None

Syntax Description

`port-setting`	Configure AP port settings
`no lan <NUMBER>`	Disable the AP LAN port
`no dot1x <authsvr> <acctsvr> <mac-auth-bypass>`	Disable authentication server, accounting server, or MAC auth bypass for the AP's 802.1X settings
`lan <NUMBER> {Arguments}`	Configure the AP LAN port.

`dot1x <authsvr> <acctsvr> <mac-auth-bypass>`	Enable authentication server, accounting server, or MAC auth bypass for the AP's 802.1X settings
`authsvr <WORD>`	Enter the RADIUS server name
`acctsvr <WORD>`	Enter the RADIUS accounting server name
`mac-auth-bypass`	Enable MAC authentication bypass for the 802.1X-enabled port

Example

```
ruckus(config-ap)# port-setting
ruckus(config-ap-model)#
```

abort

To exit the `port-setting` context without saving changes, use the `abort` command.

```
abort
```

Syntax Description

abort	Exit the context without saving changes

Defaults

None.

Example

```
ruckus(config-ap-model)# abort
No changes have been saved.
ruckus(config-ap)#
```

end

To save changes, and then exit the `port-setting` context, use the following command:

```
end
```

Syntax Description

end	Save changes, and then exit the context

Defaults

None.

Example

```
ruckus(config-ap-model)# end
ruckus(config-ap)#
```

exit

To save changes, and then exit the `config-ap-model` context, use the following command:

```
exit
```

Syntax Description

exit	Save changes, and then exit the context

Defaults

None.

Example

```
ruckus(config-ap-model)# exit
ruckus(config-ap)#
```

quit

To exit the `config-ap-model` context without saving changes, use the `quit` command.

```
quit
```

Syntax Description

quit	Exit the context without saving changes

Defaults

None.

Example

```
ruckus(config-ap-model)# quit
No changes have been saved.
ruckus(config-ap)#
```

show

To display the current port settings, use the following command:

```
show
```

Syntax Description

show	Display the current port settings

Defaults

None.

Example

```
ruckus(config)# ap 04:4f:aa:0c:b1:00
```

```
ruckus(config-ap)# port-setting
ruckus(config-ap-model)# show
PORTS:
    LAN ID:
          1:
            Enable LAN = Yes
            LAN Type= trunk
            Untag ID= 1
            Members= 1-4094
            Guest VLAN=
            Enable Dynamic VLAN= Disabled
            802.1X= disabled
            DHCP opt82= Disabled
            MLD Snooping= Disabled
            IGMP Snooping= Enabled
          2:
            Enable LAN = Yes
            LAN Type= trunk
            Untag ID= 1
            Members= 1-4094
            Guest VLAN=
            Enable Dynamic VLAN= Disabled
            802.1X= disabled
            DHCP opt82= Disabled
            MLD Snooping= Disabled
            IGMP Snooping= Enabled
ruckus(config-ap-model)#
```

lan

To enable the LAN port, use the following command:

```
lan <NUMBER>
```

Syntax Description

lan	Enable the LAN port
<NUMBER>	Specify the LAN port to enable

Defaults

Enabled.

Example

```
ruckus(config-ap-model)# lan 1
ruckus(config-ap-model)#
```

no lan

To disable the LAN port, use the following command:

```
no lan <NUMBER>
```

Syntax Description

no lan	Disable the LAN port
<NUMBER>	Specify the LAN port to disable

Defaults

None.

Example

```
ruckus(config-ap-model)# no lan 1
ruckus(config-ap-model)#
```

lan uplink

To sets the AP port type (Trunk, Access or General), use the following command:

```
lan <NUMBER> uplink <WORD>
```

Syntax Description

lan uplink	Set the LAN port type
<NUMBER>	Specify the LAN port to configure
uplink	Set the port type to the specified type
<WORD>	LAN port type (Trunk port, Access port, General port)

Defaults

For all APs other than 7025: Trunk

For 7025 LAN 5: Trunk

For 7025 LAN 1-LAN 4: Access

Example

```
ruckus(config-ap-model)# lan 1 uplink access
ruckus(config-ap-model)#
```

lan untag

To set the LAN port untag VLAN ID (native VLAN, for Trunk ports), use the following command:

```
lan <NUMBER> untag <NUMBER>
```

Syntax Description

lan untag	Set the LAN port untag VLAN ID
<NUMBER>	Specify the LAN port to configure
<NUMBER>	Set the untag VLAN ID (1~4094)

Defaults

1

Example

```
ruckus(config-ap-model)# lan 1 untag 1
ruckus(config-ap-model)#
```

lan member

To set the LAN port VLAN membership (only General ports have configurable membership; Trunk ports are members of all VLANs, and Access port membership must be the same as the Untag VLAN), use the following command:

```
lan <NUMBER> member <NUMBER>
```

Syntax Description

lan member	Set the LAN port VLAN membership
<NUMBER>	Specify the LAN port to configure
<NUMBER>	Set the VLAN membership (1~4094, range separated by hyphen, multiple VLANs separated by commas)

Defaults

1

Example

```
ruckus(config-ap-model)# lan 1 uplink general
ruckus(config-ap-model)# lan 1 member 1-10,100,200
ruckus(config-ap-model)# show
PORTS:
LAN ID:
1:
Enable LAN = Yes
LAN Type= general
Untag ID= 12
Members= 1-10,100,200
802.1X= disabled
DHCP opt82= Disabled
LAN ID:
2:
```

```
Enable LAN = Yes
LAN Type= trunk
Untag ID= 1
Members= 1-4094
802.1X= disabled
DHCP opt82= Disabled
ruckus(config-ap-model)#
```

lan opt82

To enable or disable DHCP option 82 for a LAN port, use the following command:

```
lan <NUMBER> opt82 [enabled|disabled]
```

Syntax Description

opt82	Enable or disable DHCP option 82
enabled	Enable option 82
disabled	Disable option 82

Defaults

Disabled

Example

```
ruckus(config-ap-model)# lan 1 opt82 enable
ruckus(config-ap-model)#
```

lan guest-vlan

To set the AP port to use the specified Guest VLAN ID, use the following command:

```
lan <NUMBER> guest-vlan <NUMBER>
```

lan dvlan

To enable dynamic VLAN for the port, use the following command:

```
lan <NUMBER> dvlan
```

lan dvlan disabled

To disable dynamic VLAN for the port, use the following command:

```
lan <NUMBER> dvlan disabled
```

lan dvlan enabled

To enable dynamic VLAN for the port, use the following command:

```
lan <NUMBER> dvlan enabled
```

lan dot1x

To configure 802.1X settings for a LAN port, use the following command:

```
lan <NUMBER> dot1x [disable|supplicant|auth-port-based|auth-mac-based]
```

Syntax Description

lan dot1x	Configure 802.1X settings for this port
<NUMBER>	LAN port number to configure
disabled	Disable 802.1X
supplicant	Configure this LAN port as an 802.1X supplicant
auth-port-based	Configure this LAN port as an 802.1X authenticator (port-based)
auth-mac-based	Configure this LAN port as an 802.1X authenticator (MAC-based)

Defaults

Disabled

Example

```
ruckus(config-ap-model)# lan 1 dot1x supplicant
ruckus(config-ap-model)#
```

dot1x authsvr

To configure 802.1X authentication server, use the following command:

```
dot1x authsvr <WORD>
```

Syntax Description

dot1x authsvr	Configure 802.1X authentication server
<WORD>	Name of AAA server

Defaults

None

Example

```
ruckus(config-ap-model)# dot1x authsvr radius
ruckus(config-ap-model)#
```

dot1x acctsvr

To configure 802.1X accounting server, use the following command:

```
dot1x acctsvr <WORD>
```

Syntax Description

dot1x acctsvr	Configure 802.1X accounting server
<WORD>	Name of AAA server

Defaults

None

Example

```
ruckus(config-ap-model)# dot1x acctsvr radius-acct
ruckus(config-ap-model)#
```

dot1x mac-auth-bypass

To configure 802.1X MAC authentication bypass, use the following command:

```
dot1x mac-auth-bypass
```

Syntax Description

`dot1x mac-auth-bypass`	Enable 802.1X MAC authentication bypass

Defaults

Disabled

Example

```
ruckus(config-ap-model)# dot1x mac-auth-bypass
ruckus(config-ap-model)#
```

dot1x supplicant username

To configure 802.1X supplicant user name, use the following command:

```
dot1x supplicant username <WORD>
```

Syntax Description

`dot1x supplicant username`	Configure 802.1X supplicant user name
<WORD>	Set the 802.1X supplicant user name

Defaults

None

Example

```
ruckus(config-ap-model)# dot1x supplicant username johndoe
ruckus(config-ap-model)#
```

dot1x supplicant password

To configure 802.1X supplicant password, use the following command:

```
dot1x supplicant password <WORD>
```

Syntax Description

`dot1x supplicant password`	Configure 802.1X supplicant password
<WORD>	Set the 802.1X supplicant password

Defaults None

Example

```
ruckus(config-ap-model)# dot1x supplicant password test123
ruckus(config-ap-model)#
```

dot1x supplicant mac

To set the 802.1X supplicant user name and password as the AP's MAC address, use the following command:

```
dot1x supplicant mac
```

Syntax Description

`dot1x supplicant mac`	Set the supplicant user name and password as the AP's MAC address

Defaults None

Example

```
ruckus(config-ap-model)# dot1x supplicant mac
ruckus(config-ap-model)#
```

Configure AP Policy Commands

Use the `ap-policy` commands to configure global AP policies such as automatic AP approval, limited ZD discovery, management VLAN, load balancing across APs and max clients per AP radio. To run these commands, you must first enter the `config-ap-policy` context.

ap-policy

To enter the ap-policy context and configure global AP policies, enter the following command:

```
ap-policy
```

Syntax Description

`ap-policy`	Enter config-ap-policy context and configure global AP policies

Defaults

None.

Example

```
ruckus(config)# ap-policy
ruckus(config-ap-policy)#
```

show

To display the current device policy, use the following command:

```
show
```

Syntax Description

`show`	Display the current AP policy settings

Defaults

None.

Example

```
ruckus(config-ap-policy)# show
  Automatically approve all join requests from APs= Enabled
  Limited ZD Discovery:
    Status= Disabled
  Management VLAN:
    Status= Keep AP's setting
  Balances the number of clients across adjacent APs= Disabled
  LWAPP message MTU= 1450
  Auto Recovery= 30 minutes
ruckus(config-ap-policy)#
```

ap-management-vlan

To enable the AP management VLAN and set to either "keep AP's setting" or to the specified VLAN ID, use the following command:

```
ap-management-vlan [keeping] <NUMBER>
```

Syntax Description

`ap-management-vlan`	Enable and configure the global AP management VLAN
`keeping`	Sets management VLAN to "Keep AP's setting"

<NUMBER>	Set management VLAN to the number specified

Defaults

None.

Example

```
ruckus(config-ap-policy)# ap-management-vlan keeping
The command was executed successfully.
ruckus(config-ap-policy)#
```

no ap-management-vlan

To disable the AP management VLAN, use the following command:

```
no ap-management-vlan
```

Syntax Description

no ap-management-vlan	Disable the AP management VLAN

Defaults

None.

```
ruckus(config-ap-policy)# no ap-management-vlan
```

Example

```
The command was executed successfully.
ruckus(config-ap-policy)#
```

ap-auto-approve

To enable the automatic approval of join requests from devices, use the following command:

```
ap-auto-approve
```

Syntax Description

ap-auto-approve	Enable the automatic approval of join requests from devices

Defaults

None.

Example

```
ruckus(config-ap-policy)# ap-auto-approve
The AP automatically approve policy has been updated.
```

no ap-auto-approve

To disable the automatic approval of join requests from devices, use the following command:

```
no ap-auto-approve
```

Syntax Description

`no ap-auto-approve`	Disable the automatic approval of join requests from devices

Defaults

None.

Example

```
ruckus(config-ap-policy)# no ap-auto-approve
The AP automatically approve policy has been updated.
ruckus(config-ap-policy)#
```

limited-zd-discovery

To configure devices to connect to a specific ZoneDirector and to set the primary and secondary ZoneDirector's IP addresses, use the following command:

```
limited-zd-discovery <zd-addr|zd-ip> <PRIMARY> <SECONDARY>
```

Syntax Description

`limited-zd-discovery`	Configure devices to connect to a specific ZoneDirector
`zd-addr`	Set ZoneDirector's IP/IPv6/FQDN address
`zd-ip`	Set ZoneDirector's IP/IPv6 address
`<PRIMARY>`	Address of primary ZD
`<SECONDARY>`	Address of secondary ZD

Defaults

Disabled.

Example

```
ruckus(config-ap-policy)# limited-zd-discovery zd-addr
192.168.11.100 192.168.11.200
The Limited ZoneDirector discovery function has been updated.
ruckus(config-ap-policy)# show
Automatically approve all join requests from APs= Enabled
Limited ZD Discovery:
Status= Enabled
Primary ZoneDirector ADDR= 192.168.11.100
SecondaryZoneDirector ADDR= 192.168.11.200
```

```
Prefer Primary ZoneDirector = false
Management VLAN:
Status= Disabled
Balances the number of clients across adjacent APs= Disabled
Max. clients for 11BG radio= 100
Max. clients for 11N radio= 100
LWAPP message MTU= 1450
ruckus(config-ap-policy)#
```

limited-zd-discovery prefer-primary-zd

To force the AP to prefer the primary ZoneDirector when connected (and periodically attempt to reconnect to the primary ZD when disconnected from it), use the following command:

```
limited-zd-discovery prefer-primary-zd
```

Example

```
ruckus(config-ap-policy)# limited-zd-discovery prefer-primary-zd
The Limited ZoneDirector discovery function has been updated.
ruckus(config-ap-policy)#
```

no limited-zd-discovery

To disable limited ZD discovery, use the following command:

```
no limited-zd-discovery
```

Syntax Description

`no limited-zd-discovery`	Disable limited ZD discovery

Defaults

Disabled.

Example

```
ruckus(config-ap-policy)# no limited-zd-discovery
The Limited ZoneDirector discovery function has been updated.
ruckus(config-ap-policy)#
```

limited-zd-discovery keep-ap-setting

To disallow ZoneDirector modifying AP's original primary/secondary ZD settings, use the following command:

```
limited-zd-discovery keep-ap-setting
```

Example

```
ruckus(config-ap-policy)# limited-zd-discovery keep-ap-setting
The Limited ZoneDirector discovery function has been updated.
ruckus(config-ap-policy)#
```

ap-max-clients

To set the maximum number of wireless clients that can associate with each device, use the following command:

```
ap-max-clients [11bg|11n] <NUMBER>
```

Syntax Description

ap-max-clients	Set the maximum number of clients per AP
11bg	Set the max clients for the 11bg (2.4 GHz) radio
11n	Set the max clients for the 11n (5 GHz) radio
<NUMBER>	Set to this number

Defaults

None.

Example

```
ruckus(config-ap-policy)# ap-max-clients 11n 99
The Max clients of AP management has been updated.
ruckus(config-ap-policy)#
```

ap-load-balancing

To enable load balancing across adjacent APs, use the following command:

```
ap-load-balancing
```

Syntax Description

ap-load-balancing	Enable load balancing across adjacent APs

Defaults

Disabled.

Example

```
ruckus(config-ap-policy)# ap-load-balancing
The load balancing of AP management has been updated.
ruckus(config-ap-policy)#
```

no ap-load-balancing

To disable load balancing across adjacent APs, use the following command:

```
no ap-load-balancing
```

Syntax Description

`no ap-load-balancing`	Disable load balancing across adjacent APs

Defaults

Disabled.

Example

```
ruckus(config-ap-policy)# no ap-load-balancing
The load balancing of AP management has been updated.
ruckus(config-ap-policy)#
```

lwapp-message-mtu

To configure the LWAPP message MTU size, use the following command:

```
lwapp-message-mtu <NUMBER>
```

Syntax Description

`lwapp-message-mtu`	Configure LWAPP message maximum transmit unit size
`<NUMBER>`	Set the LWAPP MTU to this number (600~1450)

Defaults

1450

Example

```
ruckus(config-ap-policy)# lwapp-message-mtu 1450
The AP Policy has been updated.
ruckus(config-ap-policy)#
```

auto-recovery

To set the value of auto recovery time (minutes) for AP reboot if AP can't connect to ZoneDirector, use the following command:

```
auto-recovery <NUMBER>
```

no auto-recovery

To disable AP auto recovery, use the following command:

```
no auto-recovery
```

vlan-qos

To configure the traffic class [Voice | Video | Data | Background] to the specific VLAN ID at the specific interface, use the following command:

```
vlan-qos <VID> <Traffic Class> <Interface Name>
```

Syntax Description

`vlan-qos`	Configure VLAN QOS settings
`<VID>`	VLAN ID
`<Traffic Class>`	Specify traffic classification (voice, video, data, background)
`<Interface Name>`	Specify interface name

Defaults

Disabled

Example

```
ruckus(config-ap-policy)# vlan-qos 10 voice eth0
The VLAN QoS function has been updated.
ruckus(config-ap-policy)#
```

no vlan-qos

To disable QOS for the specific interface, use the following command:

```
no vlan-qos <VID> <Interface Name>
```

Syntax Description

`no vlan-qos`	Disable VLAN's QOS settings
`<VID>`	VLAN ID
`<Interface Name>`	Specify interface name

Defaults

Disabled

Example

```
ruckus(config-ap-policy)# no vlan-qos all eth0
The VLAN QoS function has been updated.
ruckus(config-ap-policy)#
```

move-ap

To enter the config-ap-policy-move-ap context, use the following command:

```
move-ap
```

Example

```
ruckus(config-ap-policy)# move-ap
```

```
ruckus(config-ap-policy-move-ap)#
```

move-ap

To move an AP to the specific Primary ZD/[Secondary ZD] address from within the config-ap-policy-move-ap context, use the following command:

```
move-ap <MAC | index range> <ADDR> [<ADDR>]
```

no move-ap

To remove the address settings of move-AP from the selected APs, use the following command:

```
no move-ap <MAC | index range>
```

no move-ap-group

To remove the AP Group Name settings of move-AP from the selected APs, use the following command:

```
no move-ap-group <MAC> | <index range>
```

move-ap-group

To move an AP to the specific ZD with AP Group Name, use the following command:

```
move-ap-group <MAC | index range> <AP-GROUP-NAME>
```

no move-ap-group

To remove the AP Group Name settings of move-AP from the selected APs, use the following command:

```
no move-ap-group <MAC> | <index range>
```

timeout

To configure recovering of the APs' original Primary/Secondary ZD address if the AP can't find the desired Primary/Secondary ZD after timeout(minutes), use the following command:

```
timeout <NUMBER>
```

Syntax Description

`timeout`	Enter the timeout value (minutes) for recovering APs' original primary/secondary ZD IP.
`<NUMBER>`	Timeout value in minutes.

Example

```
ruckus(config-ap-policy-move-ap)# timeout 60
```

```
Your changes have been saved.
ruckus(config-ap-policy-move-ap)#
```

import-aplist

To import an AP list from backup files on a TFTP server, use the following command:

```
import-aplist <IP-ADDR> <FILE-NAME>
```

exit

Saves changes, and then exits the config-ap-policy-move-ap context.

abort

Exits the config-ap-policy-move-ap context without saving changes.

quit

Exits the config-ap-policy-move-ap context without saving changes.

show

Displays the AP policy settings.

Example

```
ruckus(config-ap-policy)# show
  Automatically approve all join requests from APs= Enabled
  Limited ZD Discovery:
    Status= Disabled
  Management VLAN:
    Status= Keep AP's setting
  Balances the number of clients across adjacent APs= Disabled
  Auto Recovery= 30 minutes
ruckus(config-ap-policy)#
```

Configure AP Group Commands

This section describes the commands that you can use to configure AP groups on the controller. The following commands can be executed from within the `config-apgrp` context. To show a list of commands available from within the context, type help or ?.

ap-group

To create a new AP group or configure an existing AP group and enter the `config-apgrp` context, enter the following command:

```
ap-group <WORD>
```

Syntax Description

`ap-group`	Configure an AP group
`<WORD>`	Name of the AP group

Defaults

"System Default"

Example

```
ruckus(config)# ap-group "System Default"
The AP group entry 'System Default' has been loaded. To save the
AP group, type 'end' or 'exit'.
ruckus(config-apgrp)#
```

no ap-group

To delete an AP group from the list, enter the following command:

```
no ap-group <WORD>
```

Syntax Description

`no ap-group`	Delete an AP group
`<WORD>`	Name of the AP group

Defaults

None

Example

```
ruckus(config)# no ap-group apgrp2
The AP Group 'apgrp2' has been removed.
ruckus(config)#
```

show

Displays current AP group configuration settings.

```
show
```

Defaults

None

Example

```
ruckus(config)# ap-group apgroup1
```

```
The AP group 'apgroup1' has been created. To save the AP group,
type 'end' or 'exit'.
ruckus(config-apgrp)# show
APGROUP:
       ID:
         :
           Name= apgroup1
           Description=
           Radio 11bgn:
             Channelization= Auto
             Channel= Auto
         Enable auto channel selection which select from 1,6,11= Yes
             Tx. Power= Auto
             11N only Mode= Auto
             WLAN Group= Default
             Call Admission Control= OFF
           Radio 11an:
             Channelization= Auto
             Channel= Auto
             Tx. Power= Auto
             11N only Mode= Auto
             WLAN Group= Default
             Call Admission Control= OFF
           Members:

ruckus(config-apgrp)#
```

description

To set the AP group description, use the following command:

```
description <WORD>
```

no description

To delete the AP group description, use the following command:

```
no description
```

ipmode

To set the IP addressing mode of the AP group, use the following command:

```
ipmode <WORD>
```

Syntax Description

`ipmode`	Set the IP addressing mode

<WORD>	IPv4, IPv6 or dual

Example

```
ruckus(config-apgrp)# ipmode dual
ruckus(config-apgrp)#
```

no ipmode-override

To disable the override of IP mode, use the following command:

```
no ipmode-override
```

Radio 2.4/5 GHz Commands

Use the `radio 2.4` or `radio 5` commands to configure the 2.4/5 GHz radios on all APs within an AP group.

radio

To configure radio settings for the 2.4 GHz or 5 GHz radios of an AP group, use the following command:

```
radio [2.4|5] <arguments>
```

Syntax Description

`radio`	Configure AP group radio settings
`2.4`	Configure 2.4 GHz radio
`5`	Configure 5 GHz radio
`no`	Disables settings for the specified radios in the AP group
`channel`	Set radio channel (Auto or number)
`channelization`	Set radio channel width (Auto, 20MHz or 40MHz)
`auto-channel-selection [four-channel|three-channel]`	Set auto channel selection to four-channel (1,5,9,13) or three-channel (1,6,11)
`tx-power`	Set radio transmit power (Auto, Full, 1/2, 1/4, 1/8, Min) or <NUMBER> (-1dB~-10dB)
`11n-only`	Set radio 11n-only mode to Auto or N-only
`wlan-group`	Set radio to the specified WLAN group
`admission-control`	Set the radio to use the specific call admission control airtime usage limit (%)

Defaults

Channel: Auto

Channelization: Auto

Auto-Channel Selection: Three-channel

TX Power: Auto

11n-only: Auto

WLAN group: Default

Admission Control: Off

Example

```
ruckus(config)# ap-group "System Default"
The AP group entry 'System Default' has been loaded. To save the
AP group, type 'end' or 'exit'.
ruckus(config-apgrp)# radio 2.4 channel auto
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-apgrp)# radio 5 channelization auto
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-apgrp)# radio 5 11n-only N-only
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-apgrp)# radio 5 wlan-group Default
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-apgrp)# radio 2.4 tx-power Num 1
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-apgrp)# show
APGROUP:
 ID:
 1:
 Name= System Default
 Description= System default group for Access Points
 Radio 11bgn:
 Channelization= Auto
 Channel= Auto
 Enable auto channel selection which select from 1,6,11= Yes
 Tx. Power= -1dB
 11N only Mode= Auto
 WLAN Group= Default
 Radio 11an:
 Channelization= Auto
 Channel= Auto
 Tx. Power= Auto
```

```
 11N only Mode= N-only
 WLAN Group= Default
 Members:
 MAC= 04:4f:aa:0c:b1:00
 MAC= 00:24:82:3f:14:60
 MAC= 74:91:1a:2b:ff:a0
 MAC= 00:1f:41:2a:2b:10

ruckus(config-apgrp)# end
The AP group 'System Default' has been updated.
Your changes have been saved.
ruckus(config)#
```

radio 2.4 channel auto

Sets the 2.4GHz radio to use 'Auto' channel.

radio 2.4 channel number <NUMBER>

Sets the 2.4GHz radio to use the specified channel.

radio 2.4 channelization auto

Sets the 2.4GHz radio to use 'Auto' channelization.

radio 2.4 channelization number <NUMBER>

Sets the 2.4GHz radio to use the specified channelization.

radio 2.4 auto-channel-selection four-channel

Enables the auto channel selection which always select from 1,5,9,13.

radio 2.4 auto-channel-selection three-channel

Enables the auto channel selection which always select from 1,6,11.

radio 2.4 tx-power Auto

Sets the 2.4GHz radio to use 'Auto' Tx. power setting.

radio 2.4 tx-power Full

Sets the 2.4GHz radio to use the specified Tx. power setting.

radio 2.4 tx-power 1/2

Sets the 2.4GHz radio to use the specified Tx. power setting.

radio 2.4 tx-power 1/4

Sets the 2.4GHz radio to use the specified Tx. power setting.

radio 2.4 tx-power 1/8

Sets the 2.4GHz radio to use the specified Tx. power setting.

radio 2.4 tx-power Min

Sets the 2.4GHz radio to use the specified Tx. power setting.

radio 2.4 tx-power Num

Sets the 2.4GHz radio to use the specified Tx by number from 1-10 (-1dB ~ -10dB).

radio 2.4 11n-only Auto

Sets the 2.4GHz radio to use 'Auto' 11N only mode.

radio 2.4 11n-only N-only

Sets the 2.4GHz radio to use the specified 11N only mode.

radio 2.4 wlan-group <WORD>

Assigns the 2.4GHz radio to the specified WLAN group.

radio 2.4 admission-control <VALUE>

Sets the 2.4GHz radio to use the specific call admission control airtime usage limit(%).

radio 2.4 channel-range <NUMBER-LIST>

Sets the allowed list of channels used in 2.4GHz radio.

radio 5 indoor channel auto

Sets the 5GHz radio (indoor) to use 'Auto' channel.

radio 5 indoor channel number <NUMBER>

Sets the 5GHz radio (indoor) to use the specified channel.

radio 5 indoor channel-range <NUMBER-LIST>

Sets the allowed list of indoor channels used in 5GHz radio.

radio 5 outdoor channel auto

Sets the 5GHz radio (outdoor) to use 'Auto' channel.

radio 5 outdoor channel number <NUMBER>

Sets the 5GHz radio (outdoor) to use the specified channel.

radio 5 outdoor channel-range <NUMBER-LIST>

Sets the allowed list of outdoor channels used in 5GHz radio.

radio 5 channel auto

Sets the 5GHz radio to use 'Auto' channel.

radio 5 channel number <NUMBER>

Sets the 5GHz radio to use the specified channel.

radio 5 channelization auto

Sets the 5GHz radio to use 'Auto' channelization.

radio 5 channelization number <NUMBER>

Sets the 5GHz radio to use the specified channelization.

radio 5 tx-power Auto

Sets the 5GHz radio to use 'Auto' Tx. power setting.

radio 5 tx-power Full

Sets the 5GHz radio to use the specified Tx. power setting.

radio 5 tx-power 1/2

Sets the 5GHz radio to use the specified Tx. power setting.

radio 5 tx-power 1/4

Sets the 5GHz radio to use the specified Tx. power setting.

radio 5 tx-power 1/8

Sets the 5GHz radio to use the specified Tx. power setting.

radio 5 tx-power Min

Sets the 5GHz radio to use the specified Tx. power setting.

radio 5 tx-power Num

Sets the 5GHz radio to use the specified Tx by number from 1-10 (-1dB ~ -10dB).

radio 5 11n-only Auto

Sets the 5GHz radio to use 'Auto' 11N only mode.

radio 5 11n-only N-only

Sets the 5GHz radio to use the specified 11N only mode.

radio 5 wlan-group <WORD>

Assigns the 5GHz radio to the specified WLAN group.

radio 5 admission-control <VALUE>

Sets the 5GHz radio to use the specific call admission control airtime usage limit(%).

no radio 2.4 channelization-override

Disables the override of the 2.4GHz channelization settings.

no radio 2.4 channel-range-override

Disables the override of the 2.4GHz channel range settings.

no radio 2.4 channel-override

Disables the override of the 2.4GHz channel settings.

no radio 2.4 tx-power-override

Disables the override of the 2.4GHz Tx. power settings.

no radio 2.4 11n-only-override

Disables the override of the 2.4GHz 11N only mode settings.

no radio 2.4 wlan-group-override

Disables the override of the 2.4GHz WLAN group settings.

no radio 2.4 admission-control

Disables call admission control function on the 2.4GHz radio.

no radio 2.4 admission-control-override

Disables the override of the 2.4GHz call admission control settings.

no radio 5 indoor channel-range-override

Disables the override of the 5GHz indoor channel range settings.

no radio 5 indoor channel-override

Disables the override of the 5GHz indoor channel settings.

no radio 5 outdoor channel-range-override

Disables the override of the 5GHz outdoor channel range settings.

no radio 5 outdoor channel-override

Disables the override of the 5GHz outdoor channel settings.

no radio 5 channelization-override

Disables the override of the 5GHz channelization settings.

no radio 5 tx-power-override

Disables the override of the 5GHz Tx. power settings.

no radio 5 11n-only-override

Disables the override of the 5GHz 11N only mode settings.

no radio 5 wlan-group-override

Disables the override of the 5GHz WLAN group settings.

no radio 5 admission-control

Disables call admission control function on the 5GHz radio.

no radio 5 admission-control-override

Disables the override of the 5GHz call admission control settings.

QoS Commands

Use the following commands to configure QoS settings for the AP group.

qos

Contains commands that can be executed from within the context.

qos mld-query

Contains commands that can be executed from within the context.

qos mld-query v1

Enables the mld-query v1.

qos mld-query v2

Enables the mld-query v2.

qos igmp-query

Contains commands that can be executed from within the context.

qos igmp-query v2

Enables the igmp-query v2.

qos igmp-query v3

Enables the igmp-query v3.

qos query-interval

Sets the query interval to the specified value.

```
qos query-interval <VALUE>
```

no qos mld-query v1

Disables the mld-query v1.

no qos mld-query v2

Disables the mld-query v2.

no qos igmp-query v2

Disables the igmp-query v2.

no qos igmp-query v3

Disables the igmp-query v3.

Model-Specific Commands

The following commands are used to configure model-specific settings for all APs of a certain model within an AP group.

no model-setting

To discard the model settings for this specified model, use the following command:

```
no model-setting <WORD>
```

model

To configure model-specific settings for all APs of a certain model within an AP group, use the following command:

```
model <WORD> <arguments>
```

Syntax Description

`model`	Configure AP group model-specific settings
`<WORD>`	Enter the AP model name (e.g., zf2942, zf2741, zf7025, zf7341, zf7343, zf7363, zf7761cm, zf7762, zf7762-s, zf7762-t, zf7762-ac, zf7762-s-ac, zf7762-t-ac, zf7942, zf7962).
`port-setting`	Configures the port setting for the specified AP model. Enters config-apgrp-port context. See "Configure AP Group Model-Specific Port Settings" for more information.
`status-leds`	Configures the status LEDs for the specified AP model (enable, disable).
`external-antenna`	Configures external antenna settings. See "Configure AP Group Model-Specific Antenna Settings".
`spectra-analysis`	Configures spectrum analysis per radio (2.4Ghz / 5GHz, enable / disable).

`radio-band`	Sets the radio band for the AP group (APs with radio band selection only).
`max-clients <NUMBER>`	Sets the maximum clients for the AP.
`usb-software <VID-PID>`	Selects the USB Software Vendor ID and Product ID for the AP.
`poe-out`	Configures the PoE Out ports for the specified AP model (enable, disable).
`internal-heater`	Configures the internal heater for the specified AP model (enable, disable).
`cband-channels`	Configures the C-band (5.8 GHz) channels for the specified AP model (enable, disable). (UK country code only)

Defaults

Status LEDs: Enabled

PoE Out: Disabled

Internal Heater: Disabled

C-band channels: Disabled

Example

```
ruckus(config-apgrp)# model zf7343 status-leds enable
ruckus(config-apgrp)# end
The AP group 'System Default' has been updated.
Your changes have been saved.
ruckus(config)#
```

no model override

To disable model-specific override of status LEDs, radio band, PoE-out, internal heater, C-band channels, external antennas and port settings, use the following command:

```
no model <WORD> <arguments>
```

Syntax Description

`no model`	Disable AP group model-specific override settings
`<WORD>`	Enter the AP model name (e.g., zf2741,zf2741-ext,zf2942,zf7025,zf7055,zf7321,zf7321-u,zf7341,zf7343,zf7352,zf7363,zf7372,zf7372-e,zf7351,zf7761cm,zf7762,zf7762-ac,zf7762-n,zf7762-s,zf7762-s-ac,zf7762-t,zf7781cm,zf7781cm-e,zf7781cm-s,zf7781fn,zf7781fn-e,zf7781fn-s,zf7781-m,zf7782,zf7782-e,zf7782-n,zf7782-s,zf7962,zf7982,sc8800-s,sc8800-s-ac).

`port-setting`	Disables the override of the port settings for the specified AP model.
`status-leds-override`	Disables the override of the status LEDs for this specified AP model.
`external-antenna-override`	Disables the override of external antenna settings for this specified AP model.
`radio-band-override`	Disables the override of the radio band for this specified AP model.
`usb-software-override`	Disables the override of the USB software for this specified AP model.
`poe-out-override`	Disables the override of the PoE out port for this specified AP model.
`internal-heater-override`	Disables the override of the internal heater for this specified AP model.
`cband-channels-override`	Disables the override of the 5.8GHz channels for this specified AP model.

Example

```
ruckus(config-apgrp)# no model zf7363 status-leds-override
ruckus(config-apgrp)#
```

Configure AP Group Model-Specific Antenna Settings

Use the `model <WORD> external-antenna` commands from within the `config-apgrp` context to configure model-specific external antenna settings for all APs of the specified model within the AP group. The following commands are available from within this context.

`external-antenna 2.4Ghz(11BG) enable`	Enables the external antenna setting for the 2.4GHz(11BG) radio.
`external-antenna 2.4Ghz(11BG) disable`	Disables the external antenna setting for the 2.4GHz(11BG) radio.
`external-antenna 2.4Ghz(11BG) gain`	Sets the external antenna gain for the 2.4GHz(11BG) radio.
`external-antenna 2.4Ghz(11BG) 2-antennas`	Selects the two external antennas for the 2.4GHz(11BG) radio.
`external-antenna 2.4Ghz(11BG) 3-antennas`	Selects the three external antennas for the 2.4GHz(11BG) radio.

`external-antenna 2.4Ghz(11NG) enable`	Enables the external antenna setting for the 2.4GHz(11NG) radio.
`external-antenna 2.4Ghz(11NG) disable`	Disables the external antenna setting for the 2.4GHz(11NG) radio.
`external-antenna 2.4Ghz(11NG) gain`	Sets the external antenna gain for the 2.4GHz(11NG) radio.
`external-antenna 2.4Ghz(11NG) 2-antennas`	Selects the two external antennas for the 2.4GHz(11NG) radio.
`external-antenna 2.4Ghz(11NG) 3-antennas`	Selects the three external antennas for the 2.4GHz(11NG) radio.
`external-antenna 5Ghz(11NA) enable`	Enables the external antenna setting for the 5GHz(11NA) radio.
`external-antenna 5Ghz(11NA) disable`	Disables the external antenna setting for the 5GHz(11NA) radio.
`external-antenna 5Ghz(11NA) gain`	Sets the external antenna gain for the 5GHz(11NA) radio.
`external-antenna 5Ghz(11NA) 2-antennas`	Selects the two external antennas for the 2.4GHz(11NA) radio.
`external-antenna 5Ghz(11NA) 3-antennas`	Selects the three external antennas for the 2.4GHz(11NA) radio.
`external-antenna 5Ghz(11A) enable`	Enables the external antenna setting for the 5GHz(11A) radio.
`external-antenna 5Ghz(11A) disable`	Disables the external antenna setting for the 5GHz(11A) radio.
`external-antenna 5Ghz(11A) gain`	Sets the external antenna gain for the 5GHz(11A) radio.
`external-antenna 5Ghz(11A) 2-antennas`	Selects the two external antennas for the 2.4GHz(11A) radio.
`external-antenna 5Ghz(11A) 3-antennas`	Selects the three external antennas for the 2.4GHz(11A) radio.

Configure AP Group Model-Specific Port Settings

Use the `model <WORD> port-setting` command (from the `config-apgrp` context) to enter the `config-apgrp-port` context and configure model-specific port settings for all APs of the specified model within the AP group. The following commands are available from within this context.

`port-setting`	Enters the port-setting context.
`no port-setting`	Disables the override of the global AP mode configuration.
`help`	Shows available commands.
`history`	Shows a list of previously run commands.
`abort`	Exits the config-apgrp-port context without saving changes.
`end`	Saves changes, and then exits the config-apgrp-port context.
`exit`	Saves changes, and then exits the config-apgrp-port context.
`quit`	Exits the config-apgrp-port context without saving changes.
`show`	Displays config-apgrp-port context.
`lan <NUMBER>`	Enables the AP Ethernet port.
`lan <NUMBER> uplink <WORD>`	Sets the AP port to use the specified type (trunk, access or general).
`lan <NUMBER> untag <NUMBER>`	Sets the AP port to use the specified VLAN ID(1-4094).
`lan <NUMBER> member <NUMBER>`	Sets the AP port to use the specified members(1-4094).
`lan <NUMBER> opt82 enabled`	Enables the AP port DHCP option 82 settings.
`lan <NUMBER> opt82 disabled`	Disables the AP port DHCP option 82 settings.
`lan <NUMBER> dot1x disabled`	Disables the AP port 802.1X settings.
`lan <NUMBER> dot1x supplicant`	Sets the AP port to 802.1X supplicant.
`lan <NUMBER> dot1x auth-port-based`	Sets the AP port to port-based 802.1X.
`lan <NUMBER> dot1x auth-mac-based`	Sets the AP port to mac-based 802.1X.
`lan <NUMBER> guest-vlan <WORD>`	Sets the AP port to use the specified guest VLAN ID(1-4094).

`lan <NUMBER> dvlan enabled`	`Enables the AP port dynamic VLAN settings.`
`lan <NUMBER> dvlan disabled`	`Disables the AP port dynamic VLAN settings.`
`lan <NUMBER> qos mld-snooping`	Enables the AP port MLD Snooping setting.
`lan <NUMBER> qos igmp-snooping`	Enables the AP port IGMP Snooping setting.
`dot1x supplicant mac`	Sets the username and password to use AP MAC address for AP 802.1X supplicant.
`dot1x supplicant user-name <WORD>`	Sets the username for AP 802.1X supplicant.
`dot1x supplicant user-name <WORD> password <WORD>`	Sets the password for AP 802.1X supplicant.
`dot1x authsvr <WORD>`	Sets the authentication server for AP 802.1X.
`dot1x acctsvr <WORD>`	Sets the accounting server for AP 802.1X.
`dot1x mac-auth-bypass`	Enables MAC authentication bypass (Use device MAC address as username and password).
`no lan <NUMBER>`	Disables the AP Ethernet port.
`no dot1x authsvr`	Disables the auth server settings.
`no lan <NUMBER> qos mld-snooping`	Disables the AP port MLD Snooping setting.
`no lan <NUMBER> qos igmp-snooping`	Disables the AP port IGMP snooping setting.
`no dot1x authsvr`	Disables the authentication server settings.
`no dot1x acctsvr`	Disables the accounting server settings.
`no dot1x mac-auth-bypass`	Disables the MAC authentication bypass.

Example

```
ruckus(config-apgrp)# model zf7321 port-setting
ruckus(config-apgrp-port)# show
PORTS:
    LAN ID:
          1:
            Enable LAN = Yes
            LAN Type= trunk
            Untag ID= 1
```

```
                Members= 1-4094
                Guest VLAN=
                Enable Dynamic VLAN= Disabled
                802.1X= disabled
                DHCP opt82= Disabled
                MLD Snooping= Disabled
                IGMP Snooping= Enabled
ruckus(config-apgrp-port)#
```

AP Group Membership

Use the following commands to configure AP group membership (move APs into or out of the current AP group, from within the config-apgrp context).

member

Adds the AP to the specified AP group .

member add

Adds the AP to the specified AP group .

member add mac

To add the AP to the specified AP group, use the following command:

```
member add mac <WORD>
```

member mac

To move the AP to the specified AP group, use the following command:

```
member mac <WORD>
```

member mac move-to

To move the AP to the specified AP group, use the following command:

```
member mac <WORD> move-to
```

member mac move-to system-default

To move the AP to the System Default AP group, use the following command:

```
member mac <WORD> move-to system-default
```

member mac move-to name

To move the AP to the specified AP group, use the following command:

```
member mac <WORD> move-to name <WORD>
```

Model-Specific Port Settings

This section describes the commands that you can use to configure port settings for all APs of a specific model within an AP group. The following commands can be executed from within the `config-apgrp-port` context. To show a list of commands available from within the context, type help or ?.

model port-setting

To configure the port settings for all APs of a specific model within an AP group, and enter the `config-apgrp-port` context, use the following command:

```
model <WORD> port-setting
```

Syntax Description

`model`	Configure AP group model-specific settings
`<WORD>`	Enter the AP model name (e.g., zf2942, zf2741, zf7025, zf7341, zf7343, zf7363, zf7761cm, zf7762, zf7762-s, zf7762-t, zf7762-ac, zf7762-s-ac, zf7762-t-ac, zf7942, zf7962).
`port-setting`	Configures the port setting for the specified AP model. Enters config-apgrp-port context.

Example

```
ruckus(config)# ap-group "System Default"
The AP group entry 'System Default' has been loaded. To save the
AP group, type 'end' or 'exit'.
ruckus(config-apgrp)# model zf7025 port-setting
ruckus(config-apgrp-port)#
```

abort

To exit the `config-apgrp-port` context without saving changes, use the following command:

```
abort
```

Syntax Description

`abort`	Exit the context without saving changes

Defaults

None.

Example

```
ruckus(config-apgrp-port)# abort
ruckus(config-apgrp)#
```

end

To save changes, and then exit the `config-apgrp-port` context, use the following command:

```
end
```

Syntax Description

`end`	Save changes, and then exit the context

Defaults

None.

Example

```
ruckus(config-apgrp-port)# end
ruckus(config-apgrp)#
```

exit

To save changes, and then exit the `config-apgrp-port` context, use the following command:

```
exit
```

Syntax Description

`exit`	Save changes, and then exit the context

Defaults

None.

Example

```
ruckus(config-apgrp-port)# exit
ruckus(config-apgrp)#
```

quit

To exit the `config-apgrp-port` context without saving changes, use the following command:

```
quit
```

Syntax Description

`quit`	Exit the context without saving changes

Defaults None.

Example

```
ruckus(config-apgrp-port)# quit
ruckus(config-apgrp)#
```

show

To show a device's port state, use the following command:

```
show
```

Syntax Description

show	Display the device's port state

Defaults None.

Example

```
ruckus(config-apgrp)# model zf7962 port-setting
ruckus(config-apgrp-port)# show
PORTS:
LAN ID:
1:
Enable LAN = Yes
LAN Type= trunk
Untag ID= 1
Members= 1-4094
802.1X= disabled
DHCP opt82= Disabled
LAN ID:
2:
Enable LAN = Yes
LAN Type= trunk
Untag ID= 1
Members= 1-4094
802.1X= disabled
DHCP opt82= Disabled
ruckus(config-apgrp-port)#
```

no lan

To disable a LAN port on APs in an AP group, use the following command:

```
no lan <NUMBER>
```

Syntax Description

`no lan`	Disable a specific port
`<NUMBER>`	Disable this port

Defaults

Enabled.

Example

```
ruckus(config-apgrp-port)# no lan 2
ruckus(config-apgrp-port)#
```

lan

To enable a LAN port on APs in an AP group, use the following command:

```
lan <NUMBER>
```

Syntax Description

`lan`	Enable a specific port
`<NUMBER>`	Enable this port

Defaults

Enabled.

Example

```
ruckus(config-apgrp-port)# lan 2
ruckus(config-apgrp-port)#
```

lan uplink

To set port type, use the following command:

```
lan <NUMBER> uplink <WORD>
```

Syntax Description

`lan`	Configure a specific port
`<NUMBER>`	Configure this port
`uplink`	Set the port type
`<WORD>`	Port type (Trunk port, Access port, General port)

Defaults

All AP ports other than ZF 7025: Trunk

ZF 7025 port 5: Trunk

ZF 7025 LAN 1-LAN 4: Access

Example

```
ruckus(config-apgrp)# model zf7962 port-setting
ruckus(config-apgrp-port)# lan 2 uplink access
ruckus(config-apgrp-port)# show
PORTS:
LAN ID:
1:
Enable LAN = Yes
LAN Type= trunk
Untag ID= 1
Members= 1-4094
802.1X= disabled
DHCP opt82= Disabled
LAN ID:
2:
Enable LAN = Yes
LAN Type= access
Untag ID= 1
Members= 1
802.1X= disabled
DHCP opt82= Disabled
ruckus(config-apgrp-port)#
```

lan untag

To configure untag VLAN settings for a model-specific port, use the following command:

```
lan <NUMBER> untag <NUMBER>
```

Syntax Description

`lan untag`	Configure port untag VLAN
`<NUMBER>`	Configure this port
`<NUMBER>`	Set untag VLAN to this number

Defaults

1

Example

```
ruckus(config-apgrp-port)# lan 2 untag 20
ruckus(config-apgrp-port)#
```

lan member

To set the LAN port VLAN membership (only General ports have configurable membership; Trunk ports are members of all VLANs, and Access port membership must be the same as the Untag VLAN), use the following command:

```
lan <NUMBER> member <NUMBER>
```

Syntax Description

lan member	Set the LAN port VLAN membership
<NUMBER>	Specify the LAN port to configure
<NUMBER>	Set the VLAN membership (1~4094, range separated by hyphen, multiple VLANs separated by commas)

Defaults

1

Example

```
ruckus(config-apgrp-port)# lan 2 uplink general
ruckus(config-apgrp-port)# lan 2 member 1-10,100,200
ruckus(config-apgrp-port)# show
PORTS:
LAN ID:
1:
Enable LAN = Yes
LAN Type= trunk
Untag ID= 1
Members= 1-4094
802.1X= disabled
DHCP opt82= Disabled
LAN ID:
2:
Enable LAN = Yes
LAN Type= general
Untag ID= 20
Members= 1-10,100,200
802.1X= disabled
DHCP opt82= Disabled
ruckus(config-apgrp-port)#
```

lan opt82

To enable or disable DHCP option 82 for a LAN port, use the following command:

```
lan <NUMBER> opt82 [enable|disable]
```

Syntax Description

lan opt82	Enable or disable DHCP option 82
enable	Enable option 82
disable	Disable option 82

Defaults

Disabled

Example

```
ruckus(config-apgrp-port)# lan 2 opt82 enable
ruckus(config-apgrp-port)#
```

dot1x

To enable 802.1X on ports of all APs of a specific model in an AP group, use the following command:

```
model <WORD> dot1x
lan <NUMBER> dot1x [disable|supplicant|auth-port-based|auth-mac-based|guest-vlan<NUMBER>|dvlan]
```

Syntax Description

lan dot1x	Configure 802.1X settings for this port
<NUMBER>	LAN port number to configure
disable	Disable 802.1X
supplicant	Configure this LAN port as an 802.1X supplicant
auth-port-based	Configure this LAN port as an 802.1X authenticator (port-based)
auth-mac-based	Configure this LAN port as an 802.1X authenticator (MAC-based)

Defaults

Disabled

Example

```
ruckus(config-apgrp)# model zf7025 port-setting
ruckus(config-apgrp-port)# lan 1 dot1x supplicant
ruckus(config-apgrp-port)# show
PORTS:
LAN ID:
1:
Enable LAN = Yes
LAN Type= access
Untag ID= 1
Members= 1
```

```
802.1X= supp
DHCP opt82= Disabled
```

dot1x authsvr

To configure 802.1X authentication server, use the following command:

```
dot1x authsvr <WORD>
```

Syntax Description

dot1x authsvr	Configure 802.1X authentication server
<WORD>	Name of AAA server

Defaults

None

Example

```
ruckus(config-apgrp-port)# dot1x authsvr radius
ruckus(config-apgrp-port)#
```

dot1x acctsvr

To configure 802.1X accounting server, use the following command:

```
dot1x acctsvr <WORD>
```

Syntax Description

dot1x acctsvr	Configure 802.1X accounting server
<WORD>	Name of AAA server

Defaults

None

Example

```
ruckus(config-apgrp-port)# dot1x acctsvr radius-acct
ruckus(config-apgrp-port)#
```

dot1x mac-auth-bypass

To configure 802.1X MAC authentication bypass, use the following command:

```
dot1x mac-auth-bypass
```

Syntax Description

dot1x mac-auth-bypass	Enable 802.1X MAC authentication bypass

Defaults Disabled

Example

```
ruckus(config-apgrp-port)# dot1x mac-auth-bypass
ruckus(config-apgrp-port)#
```

dot1x supplicant username

To configure 802.1X supplicant user name, use the following command:

```
dot1x supplicant username <WORD>
```

Syntax Description

`dot1x supplicant username`	Configure 802.1X supplicant user name
<WORD>	Set the 802.1X supplicant user name

Defaults None

Example

```
ruckus(config-apgrp-port)# dot1x supplicant username johndoe
ruckus(config-apgrp-port)#
```

dot1x supplicant password

To configure 802.1X supplicant password, use the following command:

```
dot1x supplicant password <WORD>
```

Syntax Description

`dot1x supplicant password`	Configure 802.1X supplicant password
<WORD>	Set the 802.1X supplicant password

Defaults None

Example

```
ruckus(config-apgrp-port)# dot1x supplicant password test123
ruckus(config-apgrp-port)#
```

dot1x supplicant mac

To set the 802.1X supplicant user name and password as the AP's MAC address, use the following command:

```
dot1x supplicant mac
```

Syntax Description

`dot1x supplicant mac`	Set the supplicant user name and password as the AP's MAC address

Defaults None

Example

```
ruckus(config-apgrp-port)# dot1x supplicant mac
ruckus(config-apgrp-port)#
```

no dot1x

To disable 802.1X settings for an AP model, use the following command:

```
no dot1x [authsvr] [acctsvr] [mac-auth-bypass]
```

Syntax Description

`no dot1x`	Disable dot1x settings for the AP
authsvr	Disable authentication server
acctsvr	Disable accounting server
mac-auth-bypass	Disable MAC authentication bypass

Defaults None

Example

```
ruckus(config-apgrp-port)# no dot1x authsvr
ruckus(config-apgrp-port)#
```

lan guest-vlan

To set the AP port to use the specified guest VLAN ID(1-4094), use the following command:

```
lan <NUMBER> guest-vlan <WORD>
```

lan dvlan

To enable/disable dynamic VLAN for the AP port, use the following command:

```
lan <NUMBER> dvlan [enabled | disabled]
```

lan qos

To set the AP port QoS settings, use the following command:

```
lan <NUMBER> qos
```

lan qos mld-snooping

To enable MLD snooping for the port, use the following command:

```
lan <NUMBER> qos mld-snooping
```

lan qos igmp-snooping

To enable IGMP snooping for the port, use the following command:

```
lan <NUMBER> qos igmp-snooping
```

no lan qos

To disable QoS settings for the port, use the following command:

```
no lan <NUMBER> qos
```

no lan qos mld-snooping

To disable MLD snooping on the port, use the following command:

```
no lan <NUMBER> qos mld-snooping
```

no lan qos igmp-snooping

To disable IGMP snooping on the port, use the following command:

```
no lan <NUMBER> qos igmp-snooping
```

no dot1x

To disable 802.1x settings for the port, use the following command:

```
no dot1x
```

no dot1x authsvr

To disable the authentication server settings, use the following command

```
no dot1x authsvr
```

no dot1x acctsvr

To disable the accounting server settings, use the following command:

```
no tod1x acctsvr
```

no dot1x mac-auth-bypass

To disable MAC authentication bypass, use the following command:

no dot1x mac-auth-bypass

Configure Certificate Commands

Use the `config-certificate` commands to restore the default ZoneDirector certificate or to regenerate the private key. To run these commands, you must first enter the `config-certificate` context.

quit

To exit the `config-certificate` context without saving changes, use the `quit` command.

```
quit
```

Syntax Description

quit	Exit the certificate settings without saving changes

Defaults

None.

Example

```
ruckus(config-certificate)# quit
No changes have been saved.
```

restore

To restore the default ZoneDirector certificate and private key, use the following command.

```
restore
```

Syntax Description

restore	Restore the default ZoneDirectory certificate and private key. The restore process will be completed after ZoneDirector is rebooted.

Defaults

None.

Example

```
ruckus(config-certificate)# restore
ZoneDirector will restart now to apply the changes in the certificate
settings. If you want to configure other settings, log in again
after ZoneDirector has completed restarting.
```

re-generate-private-key

To regenerate the ZoneDirector private key, use the following command:

```
re-generate-private-key {1024|2048}
```

Syntax Description

re-generate-private-key	Regenerate the ZoneDirector private key
{1024|2048}	Specify the length of the private key as either `1024` or `2048`.

Defaults

None.

Example

```
ruckus(config-certificate)# re-generate-private-key 1024
ZoneDirector will restart now to apply the changes in the certificate
settings. If you want to configure other settings, log in again
after ZoneDirector has completed restarting.
The operation doesn't execute successfully. Please try again.
```

Configure Hotspot Redirect Settings

To configure Hotspot redirect settings, use the following command:

hotspot_redirect_https

To enable Hotspot redirect, use the following command:

```
hotspot_redirect_https
```

Defaults

None.

Example

```
ruckus(config)# hotspot_redirect_https
/bin/hotspot_redirect_https enable
ruckus(config)#
```

no hotspot_redirect_https

To disable Hotspot redirect, use the following command:

```
no hotspot_redirect_https
```

Defaults

None.

Example

```
ruckus(config)# no hotspot_redirect_https
/bin/hotspot_redirect_https disable
ruckus(config)#
```

no blocked-client

To remove a blocked client from the blocked clients list, use the following command:

```
no blocked-client <MAC>
```

Defaults

None.

Example

```
ruckus(config)# no blocked-client dc:2b:61:13:f7:72
The L2 ACL 'dc:2b:61:13:f7:72' has been deleted.
ruckus(config)#
```

Configure Layer 2 Access Control Commands

Use the `layer2 access control` commands to configure the Layer 2 Access Control List settings. To run these commands, you must first enter the `config-l2acl` context.

To enter the `config-l2acl` context, run this command:

```
ruckus# config
ruckus(config)# l2acl L2ACL-policy
ruckus(config-l2acl-L2ACL-policy)#
```

abort

To exit the `config-l2acl` context without saving changes, use the following command:

```
abort
```

Syntax Description

abort	Exit the `config-l2acl` context without saving changes

Defaults

None.

Example

```
ruckus(config-l2-acl)# abort
No changes have been saved.
ruckus(config)#
```

end

To save changes, and then exit the `config-l2acl` context, use the following command:

```
end
```

Syntax Description

end	Save changes and exit the `config-l2acl` context

Defaults

None.

Example

```
ruckus(config-l2-acl)# end
The L2 ACL entry has saved successfully.
Your changes have been saved.
ruckus(config)#
```

exit

To save changes, and then exit the `config-l2acl` context, use the following command:

```
exit
```

Syntax Description

exit	Save changes and exit the `config-l2acl` context

Defaults

None.

Example

```
ruckus(config-l2-acl)# exit
The L2 ACL entry has saved successfully.
Your changes have been saved.
ruckus(config)#
```

quit

To exit the `config-l2acl` context without saving changes, use the following command:

```
quit
```

Syntax Description

quit	Exit the `config-l2acl` context without saving changes

Defaults

None.

Example

```
ruckus(config-l2-acl)# abort
No changes have been saved.
ruckus(config)#
```

show

To displays the L2 ACL settings, use the `show` command. You must run this command from within the `config-l2acl` context.

```
show
```

Syntax Description

show	Display the Layer 2 access control list settings

Defaults

None.

Example

```
ruckus(config-l2-acl)# show
L2/MAC ACL:
ID:
3:
Name= test
Description=
Restriction: Deny only the stations listed below
Stations:
MAC Address= 00:01:02:34:44:55
MAC Address= 00:01:02:34:44:56
```

no acl

To delete an L2 ACL, use the following command:

```
no acl {ACL name}
```

Syntax Description

no acl	Delete an existing ACL
{ACL name}	Delete this ACL

Defaults

None.

Example

```
ruckus# config
ruckus(config)# no acl L2_ACL_NAME
The L2 ACL 'L2_ACL_NAME' has been deleted.
```

acl

To create a new L2 ACL entry or update an existing entry, use the following command:

```
acl {ACL name}
```

Syntax Description

acl	Create a new ACL
{ACL name}	Assign this name to the new ACL

Defaults

None.

Example

```
ruckus# config
ruckus(config)# l2acl L2_ACL_NAME
The L2 ACL entry 'L2_ACL_NAME' has been created.
ruckus(config-l2acl-L2_ACL_NAME)#
```

name

To rename an L2 ACL entry, use the following command:

```
name <WORD>
```

Syntax Description

name	Sets the L2 ACL entry name.
<WORD>	Rename the ACL to this name.

Defaults

None.

Example

```
ruckus# config
ruckus(config)# l2acl L2_ACL_NAME
The L2 ACL entry 'L2_ACL_NAME' has been created.
ruckus(config-l2acl-L2_ACL_NAME)# name L2_ACL_New_Name
The command was executed successfully.
```

description

To set the description of an L2 ACL entry, use the following command:

```
description <WORD>
```

Syntax Description

description <WORD>	Set the L2 ACL description.

Defaults

None.

Example

```
ruckus# config
ruckus(config)# l2acl L2_ACL_NAME
The L2 ACL entry 'L2_ACL_NAME' has been created.
ruckus(config-l2acl-L2_ACL_NAME)# description Description-123
The command was executed successfully.
```

add-mac

To add a MAC address to the L2 ACL, use the following command:

```
add-mac <MAC>
```

Syntax Description

add mac	Add a MAC address to the ACL
<MAC>	Add this MAC address

Defaults

None.

Example

```
ruckus# config
ruckus(config)# l2acl L2_ACL_NAME
The L2 ACL entry 'L2_ACL_NAME' has been created.
ruckus(config-l2acl-L2_ACL_NAME)# add mac 00:11:22:33:44:55
The station '00:11:22:33:44:55' has been added to the ACL.
ruckus(config-l2acl-L2_ACL_NAME)#
```

mode allow

To set the ACL mode to 'allow', use the following command:

```
mode allow
```

Syntax Description

mode allow	Set the ACL mode to allow

Defaults

None.

Example

```
ruckus# config
ruckus(config)# l2acl L2_ACL_NAME
The L2 ACL entry 'L2_ACL_NAME' has been created.
ruckus(config-l2acl-L2_ACL_NAME)# mode allow
The command was executed successfully.
```

mode deny

To set the ACL mode to 'deny', use the following command:

```
mode deny
```

Syntax Description

mode allow	Set the ACL mode to deny

Defaults

None.

Example

```
ruckus# config
ruckus(config)# l2acl L2_ACL_NAME
The L2 ACL entry 'L2_ACL_NAME' has been created.
ruckus(config-l2acl-L2_ACL_NAME)# mode deny
The command was executed successfully.
```

del-mac

To delete a MAC address from an L2 ACL, use the following command:

```
del-mac <MAC>
```

Syntax Description

del-mac	Delete a MAC address from the ACL
<MAC>	Delete this <MAC>

Defaults

None.

Example

```
ruckus(config-l2-acl)# del-mac 00:01:02:34:44:55
The station '00:01:02:34:44:55' has been removed from the ACL.
ruckus(config-l2-acl)# del-mac 00:01:02:34:44:55
The station '00:01:02:34:44:55' could not be found. Please check
the spelling, and then try again.
```

Configure Layer 3 Access Control Commands

Use the `l3acl` commands to configure the Layer 3 Access Control List settings. To run these commands, you must first enter the `config-l3acl or config-l3acl-ipv6` context.

l3acl

To enter the `config-l3acl` context, run this command:

```
l3acl <WORD>
```

Syntax Description

l3acl	Create or configure a Layer 3 Access Control List
<WORD>	Name of the L3 ACL

Defaults

None.

Example

```
ruckus(config)# l3acl "ACL 1"
The L3/L4/IP ACL entry 'ACL 1' has been created.
ruckus(config-l3acl)#
```

l3acl-ipv6

To enter the `config-l3acl-ipv6` context, run this command:

```
l3acl-ipv6 <WORD>
```

Syntax Description

l3acl-ipv6	Create or configure a Layer 3 Access Control List
<WORD>	Name of the L3 ACL

Defaults

None.

Example

```
ruckus(config)# l3acl-ipv6 "ACL 2"
The L3/L4/IPv6 ACL entry 'ACL 2' has been created.
ruckus(config-l3acl-ipv6)#
```

no l3acl

To delete an L3/L4 ACL entry, use the following command:

```
no l3acl <WORD>
```

Syntax Description

no l3acl	Delete a Layer 3 ACL
<WORD>	Name of the L3 ACL

Defaults

None.

Example

```
ruckus(config)# no l3acl "ACL test"
The L3/L4/IP ACL 'ACL test' has been deleted.
ruckus(config)#
```

abort

To exit the `config-l3acl` context without saving changes, use the following command:

```
abort
```

Syntax Description

abort	Exit the context without saving changes

Defaults

None.

Example

```
ruckus(config-l3acl)# abort
No changes have been saved.
ruckus(config)#
```

end

To save changes, and then exit the config-l3acl context, use the following command:

```
end
```

Syntax Description

end	Save changes and exit the context

Defaults

None.

Example

```
ruckus(config-l3acl)# end
The L3/L4/IP ACL entry has saved successfully.
Your changes have been saved.
ruckus(config)#
```

exit

To save changes, and then exit the `config-l3acl` context, use the following command:

```
exit
```

Syntax Description

exit	Save changes and exit the context

Defaults

None.

Example

```
ruckus# config-l3acl
ruckus(config-l3acl)# exit
Your changes have been saved.
```

quit

To exit the `config-l3acl` context without saving changes, use the following command:

```
quit
```

Syntax Description

quit	Exit the context without saving changes

Defaults

None.

Example

```
ruckus(config-l3acl)# quit
No changes have been saved.
ruckus(config)#
```

show

To display the L3ACL settings, use the `show` command. You must run this command from within the `config-l3acl` context.

```
show
```

Syntax Description

show	Display the Layer 3 access control list settings

Defaults

None.

Example

```
ruckus(config-l3acl)# show
L3/L4/IP ACL:
```

```
ID:
3:
Name= test_newname
Description= justfortestCLI
Default Action if no rule is matched= Deny all by default
Rules:
Order= 1
Description=
Type= Allow
Destination Address= Any
Destination Port= 53
Protocol= Any
Order= 2
Description=
Type= Allow
Destination Address= Any
Destination Port= 67
Protocol= Any
```

name

To set the name of anL3/L4/IP ACL entry, use the following command:

```
name <WORD>
```

Syntax Description

name	Set the name of anL3/L4/IP ACL entry
<WORD>	Name of the L3/L4/IP ACL entry

Defaults

None.

Example

```
ruckus(config-l3acl)# name test_newname
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

description

To set the description of an L3/L4/IP ACL entry, use the following command:

```
description <WORD>
```

Syntax Description

description	Set the L3/L4/IP ACL entry description
<WORD>	Set to this description

Defaults None.

Example

```
ruckus(config-l3acl)# description justfortestCLI
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

mode allow

To set the ACL mode to 'allow', use the following command:

```
mode allow
```

Syntax Description

mode	Set the ACL mode
allow	Set the mode to 'allow'

Defaults None.

Example

```
ruckus(config-l3acl)# mode allow
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

mode deny

To set the ACL mode to 'deny', use the following command:

```
mode deny
```

Syntax Description

mode	Set the ACL mode
deny	Set the mode to 'deny'

Defaults None.

Example

```
ruckus(config-l3acl)# mode deny
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

no rule-order

To delete a rule from the L3/L4/IP ACL, use the following command:

```
no rule-order <NUMBER>
```

Syntax Description

no rule-order	Delete a rule from the L3/L4/IP ACL
<NUMBER>	Delete this rule ID

Defaults None.

Example

```
ruckus(config-l3acl)# no rule-order 3
The rule '3' has been removed from the ACL.
```

rule-order

To create or modify a rule in the L3/L4/IP ACL, use the following command:

```
rule-order <NUMBER>
```

Syntax Description

rule-order	Create a new rule or modify an existing one
<NUMBER>	Create or modify this rule ID

Defaults None.

Example For example, to set the current rule as the third ACL rule to apply, use the following command:

```
ruckus(config-l3acl)# rule-order 3
ruckus(config-l3acl-rule)#
```

Layer 3 Access Control Rule Commands

Use the `l3acl-rule` commands to configure the Layer 3/Layer 4/IP Access Control List rules. To run these commands, you must first enter the `config-l3acl-rule` context. To enter the `config-l3acl-rule` context, run this command:

```
rule-order <NUMBER>
```

end

To save changes, and then exit the `config-l3acl-rule` context, use the following command:

```
end
```

Syntax Description

end	Save changes, and then exit the context

Defaults None.

Example

```
ruckus(config-l3acl-rule)# end
ruckus(config-l3acl)#
```

exit

To save changes, and then exit the `config-l3acl-rule` context, use the following command:

```
exit
```

Syntax Description

exit	Save changes, and then exit the context

Defaults

None.

Example

```
ruckus(config-l3acl-rule)# exit
ruckus(config-l3acl)#
```

order

To set the L3/L4/IP ACL rule order, use the following command:

order <NUMBER>

Example

```
ruckus(config-l3acl-rule)# order 1
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-l3acl-rule)#
```

description

To set the description of an L3/L4/IP ACL rule, use the following command:

```
description <WORD>
```

Syntax Description

description	Set the L3/L4/IP ACL rule description
<WORD>	Set to this description

Defaults

None.

Example

```
ruckus(config-l3acl-rule)# description thirdl3rule
```

```
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

type allow

To set the ACL rule type to 'allow', use the following command:

```
type allow
```

Syntax Description

type	Set the ACL rule type
allow	Set the rule type to 'allow'

Defaults

None.

Example

```
ruckus(config-l3acl-rule)# type allow
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

type deny

To set the ACL rule type to 'deny', use the following command:

```
type deny
```

Syntax Description

type	Set the ACL rule type
deny	Set the rule type to 'deny'

Defaults

None.

Example

```
ruckus(config-l3acl-rule)# type deny
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

destination address

To set the destination address of the rule, use the following command:

```
destination address <IP-ADDR/WORD>
```

Syntax Description

destination address	Set the destination address of the rule
IP-ADDR/WORD	Set the destination to this IP address

Defaults None.

Example

```
ruckus(config-l3acl-rule)# destination address 192.168.1.22
The destination IP address is invalid. Please enter 'Any' or check
the IP address(for example:192.168.0.1/24), and then please try
again.
ruckus(config-l3acl-rule)# destination address 192.168.1.22/24
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

destination port

To set the destination port of the rule, use the following command:

```
destination port <NUMBER/WORD>
```

Syntax Description

destination port	Set the destination port of the rule
<NUMBER/WORD>	Set the destination to this port number

Defaults None.

Example

```
ruckus(config-l3acl-rule)# destination port 580
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

protocol

To set the protocol for the rule, use the following command:

```
protocol <NUMBER/WORD>
```

Syntax Description

protocol	Set the protocol for the rule
<NUMBER/WORD>	Set to this protocol

Defaults None.

Example

```
ruckus(config-l3acl-rule)# protocol tcp
The protocol must be a number between 0 and 254.
ruckus(config-l3acl-rule)# protocol Any
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

show

To display L3/L4/IP ACL settings, use the following command:

```
show
```

Layer 3 IPv6 Access Control List Commands

Use the `l3acl-ipv6` command to configure the IPv6 Layer 3/Layer 4/IP Access Control List. To run these commands, you must first enter the `config-l3acl` context.

l3acl-ipv6

To enter the `config-l3acl-ipv6` context, run this command:

```
l3acl-ipv6 <NUMBER>
```

abort

Exits the config-l3acl-ipv6 context without saving changes.

end

Saves changes, and then exits the config-l3acl-ipv6 context.

exit

Saves changes, and then exits the config-l3acl-ipv6 context.

quit

Exits the config-l3acl-ipv6 context without saving changes.

name

Sets the L3/L4/IPv6 ACL entry name.

description

Sets the L3/L4/IPv6 ACL entry description.

mode allow

Sets the ACL mode to 'allow'.

mode deny

Sets the ACL mode to 'deny'.

no rule-order

Deletes a rule name from the L3/L4/IPv6 ACL.

rule-order

Creates a new L3/L4/IPv6 ACL rule or modifies an existing entry rule.

Configure L3 IPv6 Rule Commands

Use the `l3acl-ipv6-rule` commands to configure the IPv6 Layer 3/Layer 4/IP Access Control List rules. To run these commands, you must first enter the `config-l3acl-ipv6-rule` context. To enter the `config-l3acl-ipv6-rule` context, run this command:

```
rule-order <NUMBER>
```

end

Saves changes, and then exits the config-l3acl-ipv6-rule context.

exit

Saves changes, and then exits the config-l3acl-ipv6-rule context.

order

Sets the L3/L4/IPv6 ACL rule order.

description

Sets the L3/L4/IPv6 ACL rule description.

type allow

Sets the ACL rule type to 'allow'.

type deny

Sets the ACL rule type to 'deny'.

destination

Contains commands that can be executed from within the context.

destination address

Sets the destination address of a L3/L4/IPv6 ACL rule.

destination port

Sets the destination port of a L3/L4/IPv6 ACL rule.

protocol

Sets the protocol of a L3/L4/IPv6 ACL rule.

icmpv6-type Any

Sets the icmpv6 type of a L3/L4/IPv6 ACL rule.

icmpv6-type number

Sets the icmpv6 type of a L3/L4/IPv6 ACL rule.

show

Displays L3/L4/IPv6 ACL settings.

Configure Precedence Policy Commands

Use the prece commands to configure precedence policy settings. Precedence policies are used to define the order in which VLAN and rate limiting policies are applied when the WLAN settings, AAA server configuration or Device Policy settings conflict.

To run these commands, you must first enter the `config-prece` context.

prece

To create or modify a precedence policy, use the following command:

```
prece <WORD>
```

Enters the config-prece context. To save changes and exit the context, type exit or end. To exit the context without saving changes, type abort.

Example

```
ruckus(config)# prece precedence1
```

```
The Precedence Policy entry 'precedence1' has been created.
ruckus(config-prece)#
```

name

Sets the Precedence Policy entry name.

description

Sets the Precedence Policy entry description.

Configure Precedence Policy Rule Commands

Use the following commands to configure precedence policy rules.

rule

Creates a new Precedence Policy rule or modifies an existing entry rule. Enters the `config-prece-rule` context.

```
rule <NUMBER>
```

Syntax Description

rule	Create a rule and enter the rule creation context.
<NUMBER>	Enter the rule number (1-2). Each precedence policy can have up to two rules.
description	Sets the Precedence Policy rule description.
order <WORD>	Sets the order of a Precedence Policy rule. The default order is AAA, Device Policy, WLAN.
show	Displays precedence policy settings.

Example

```
ruckus(config)# prece precedence1
The Precedence Policy entry 'precedence1' has been created.
ruckus(config-prece)# rule 1
ruckus(config-prece-rule)# order "Device Policy" "WLAN" "AAA"
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-prece-rule)# end
ruckus(config-prece)# show
Precedence Policy:
  ID:
    :
      Name= precedence1
      Description=
```

```
        Rules:
          1:
            Description=
            Attribute = vlan
            Order = Device Policy,WLAN,AAA
          2:
            Description=
            Attribute = rate-limit
            Order = AAA,Device Policy,WLAN

ruckus(config-precе)#
ruckus(config-precе)# end
The Precedence Policy entry has saved successfully.
Your changes have been saved.
```

no precе

To delete a precedence policy entry, use the following command:

```
no precе <WORD>
```

Configure Device Policy Commands

Use the device policy commands to configure access control and rate limiting policies based on client type. To run these commands, you must first enter the `config-dvc-pcy` context.

dvcpcy

To create a device policy or edit an existing device policy, enter the following command:

```
dvcpcy <WORD>
```

Syntax Description

show	Display device policy settings.
name <WORD>	Set the device policy entry name.
description <WORD>	Sets the device policy entry description.
mode <WORD>	Sets the device policy entry default mode (allow or deny).
no <NUMBER>	Delete a rule.
rule <NUMBER>	Create or modify a rule. Enter the config-dvc-pcy-rule context. You can create up to nine rules per access policy (one for each OS/Type).

Defaults

None.

Example

```
ruckus(config)# dvcpcy devpcy1
The Device Policy entry 'devpcy1' has been loaded. To save the
Device Policy entry, type end or exit.
ruckus(config-dvc-pcy)# name device_policy_1
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-dvc-pcy)# description "deny iOS"
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-dvc-pcy)# rule 1
ruckus(config-dvc-pcy-rule)# type deny
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-dvc-pcy-rule)# devinfo "Apple IOS"
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-dvc-pcy-rule)# vlan none
The command was executed successfully. To save the changes, type
'end' or 'exit'.

ruckus(config-dvc-pcy-rule)# rate-limit uplink 10 downlink 10
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-dvc-pcy-rule)# end
ruckus(config-dvc-pcy)# show
Device Policy:
  ID:
    1:
      Name= device_policy_1
      Description= deny iOS
      Default Mode= deny
      Rules:
        1:
          Description=
          OS/Type = Apple iOS
          Type= deny
          VLAN = Any
          Rate Limiting Uplink = 10.00Mbps
          Rate Limiting Downlink = 10.00Mbps

ruckus(config-dvc-pcy)# end
```

```
The Device Policy entry has saved successfully.
Your changes have been saved.
ruckus(config)# show dvcpcy
Device Policy:
  ID:
    2:
      Name= device_policy_1
      Description= deny iOS
      Default Mode= deny
      Rules:
        1:
          Description=
          OS/Type = Apple iOS
          Type= deny
          VLAN = Any
          Rate Limiting Uplink = 10.00Mbps
          Rate Limiting Downlink = 10.00Mbps


ruckus(config)#
```

rule

Use the rule command from within the config-dvc-pcy context to create or edit a device policy rule and enter the config-dvc-pcy-rule context. Up to 9 rules can be created per device policy.

Syntax Description

rule	Create or edit a device policy rule. Enter the config-dvc-pcy-rule context.
description <WORD>	Set the Device Policy rule description.
devinfo <WORD>	Set the operating system type of a device policy rule.
type <WORD>	Set the device policy rule type (allow or deny).
vlan <NUMBER>	Set the VLAN ID to the number specified or "none."
rate-limit uplink <NUMBER> downlink <NUMBER>	Set the rate limiting uplink and downlink speeds in mbps (valid values are 0.10, 0.20~20 in increments of 0.25 mbps).
no rate-limit	Set rate limiting to disabled.

Example

```
ruckus(config-dvc-pcy)# rule 2
ruckus(config-dvc-pcy-rule)# description "rate limit gaming
devices"
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-dvc-pcy-rule)# devinfo "Gaming"
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-dvc-pcy-rule)# type allow
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-dvc-pcy-rule)# vlan none
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-dvc-pcy-rule)# rate-limit uplink 0.1 downlink 0.1
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-dvc-pcy-rule)# end
ruckus(config-dvc-pcy)# show
Device Policy:
  ID:
    2:
      Name= device_policy_1
      Description= deny iOS
      Default Mode= deny
      Rules:
        1:
          Description=
          OS/Type = Apple iOS
          Type= deny
          VLAN = Any
          Rate Limiting Uplink = 10.00Mbps
          Rate Limiting Downlink = 10.00Mbps
        2:
          Description= rate limit gaming devices
          OS/Type = Gaming
          Type= allow
          VLAN = Any
          Rate Limiting Uplink = 0.10Mbps
          Rate Limiting Downlink = 0.10Mbps
```

```
ruckus(config-dvc-pcy)#
```

no dvcpcy

To delete a device policy, use the following command:

```
no dvcpcy <WORD>
```

Configure Load Balancing Commands

Use the load-balancing commands to configure the controller's load balancing settings. To run these commands, you must first enter the `config-load-balancing` context.

load-balancing

To enable load-balancing and enter the config-load-balancing context, use the following command:

```
load-balancing
```

Example

```
ruckus(config)# load-balancing
ruckus(config-load-balancing)#
```

abort

To exit the `config-load-balancing` context without saving changes, use the `abort` command.

```
abort
```

Syntax Description

abort	Exit the service settings without saving changes

Defaults

None.

end

To save changes, and then exit the `config-load-balancing` context, use the following command:

```
end
```

Syntax Description

end	Save changes, and then exit the context

Defaults

None.

exit

To save changes, and then exit the `config-load-balancing` context, use the following command:

```
exit
```

Syntax Description

exit	Save changes, and then exit the context

Defaults

None.

quit

To exit the `config-load-balancing` context without saving changes, use the `quit` command.

```
quit
```

Syntax Description

quit	Exit the context without saving changes

Defaults

None.

adj-threshold

To configure the adjacent threshold for load balancing, use the following command:

```
adj-threshold [wifi0|wifi1] <NUMBER>
```

Syntax Description

adj-threshold	Configure the adjacent threshold for load balancing
wifi0, wifi1	Configure this interface
<NUMBER>	Set the adjacent threshold value (1~100)

Defaults

Wifi0: 38

Wifi1: 50

weak-bypass

To configure the weak bypass for load balancing, use the following command:

```
weak-bypass [wifi0|wifi1] <NUMBER>
```

Syntax Description

weak-bypass	Configure the weak bypass for load balancing
wifi0, wifi1	Configure this interface
<NUMBER>	Set the weak-bypass value (1~100)

Defaults 20

strong-bypass

To configure the strong bypass for load balancing, use the following command:

```
strong-bypass [wifi0|wifi1] <NUMBER>
```

Syntax Description

strong-bypass	Configure the strong bypass for load balancing
wifi0, wifi1	Configure this interface
<NUMBER>	Set the strong-bypass value (1~100)

Defaults 50

act-threshold

To configure the activation threshold for load balancing, use the following command:

```
act-threshold [wifi0|wifi1] <NUMBER>
```

Syntax Description

act-threshold	Configure the activation threshold for load balancing.
wifi0, wifi1	Configure this interface.
<NUMBER>	Set the activation threshold value (1~100).

Example

```
ruckus(config-load-balancing)# act-threshold wifi0 50
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-load-balancing)#
```

new-trigger

To configure new trigger threshold (1-100), use the following command:

```
new-trigger [wifi0|wifi1] <NUMBER>
```

Syntax Description

new-trigger	Configure a new trigger threshold for the specified interface.
wifi0, wifi1	Configure this interface.
<NUMBER>	Set the new trigger threshold value (1~100).

Example

```
ruckus(config-load-balancing)# new-trigger wifi0 3
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-load-balancing)#
```

headroom

To configure headroom settings for the specified interface, use the following command:

```
headroom [wifi0|wifi1] <NUMBER>
```

Syntax Description

headroom	Configure headroom for the specified interface.
wifi0, wifi1	Configure this interface.
<NUMBER>	Set the headroom value (1~100).

Example

```
ruckus(config-load-balancing)# headroom wifi0 3
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-load-balancing)#
```

show

To display the current service settings, use the following command:

```
show
```

Syntax Description

show	Display the current service settings

Defaults

None.

Example

```
ruckus(config-load-balancing)# show
Load Balancing:
  Status= Disabled
  Radio:
    0:
```

```
    AdjacentThreshold= 50
    WeakBypass= 33
    StrongBypass= 55
    ActivationThreshold= 1
    NewTrigger= 3
    Headroom= 3

  1:
    AdjacentThreshold= 43
    WeakBypass= 35
    StrongBypass= 55
    ActivationThreshold= 10
    NewTrigger= 3
    Headroom= 3


ruckus(config-load-balancing)#
```

no load-balancing

To disable load balancing settings, use the following command:

```
no load-balancing
```

Configure STP Commands

stp

To enable Spanning Tree Protocol, use the following command:

```
stp
```

no stp

To disable Spanning Tree Protocol, use the following:

```
no stp
```

Configure System Commands

Use the `sys` or `system` command to configure the controller's system settings, including its host name, FlexMaster server, NTP server, SNMP, and QoS settings. To run these commands, you must first enter the `config-sys` context.

system

To enter the `config-sys` context and configure system settings, use the following command:

```
system
```

Example

```
ruckus(config)# system
ruckus(config-sys)#
```

dot11-country-code

To set the controller's country code, use the following command:

```
dot11-country-code <COUNTRY-CODE>
```

Syntax Description

`dot11-country-code`	Configure the controller's country code setting
`<COUNTRY-CODE>`	Set the country code to this value

Defaults

None.

Example

To set the country code to US, enter the following command:

```
ruckus# config
ruckus(config)# system
ruckus(config-sys)# dot11-country-code US
The country code settings have been updated.
ruckus(config-sys)#
```

hostname

To set the system hostname, use the following command:

```
hostname
```

Syntax Description

`hostname`	Set the controller's system hostname

Defaults None

Example

```
ruckus(config-sys)# hostname ruckus-xjoe
The system identity/hostname settings have been updated.
```

Interface Commands

Use the `interface` commands to configure the controller's IP address and VLAN settings. To run these commands, you must first enter the `config-sys-if` context.

interface

To enter the `config-sys-if` context and configure IP address and VLAN settings, use the following command:

```
interface
```

Example

```
ruckus(config-sys)# interface
ruckus(config-sys-if)#
```

ip enable

To enable IPv4 addressing, use the following command:

```
ip enable
```

ip route gateway

To set the controller's gateway IP address, use the following command:

```
ip route gateway <GATEWAY-ADDR>
```

Syntax Description

ip route gateway	Configure the controller's gateway IP address
`<GATEWAY-ADDR>`	Set the controller' gateway IP address to this value

Defaults None.

Example

```
ruckus# config
ruckus(config)# system
ruckus(config-sys)# interface
ruckus(config-sys-if)# ip route gateway 192.168.0.1
The command was executed successfully.
```

ip name-server

To set the controller's DNS servers, use the ip name-server command. Use a space to separate the primary and secondary DNS servers.

```
ip name-server <DNS-ADDR> [<DNS-ADDR>]
```

Syntax Description

ip name-server	Configure the controller's DNS server address or addresses
DNS-ADDR	Set the DNS server address to this value. If entering primary and secondary DNS server addresses, use a space to separate the two addresses.

Defaults

None.

Example

```
ruckus# config
ruckus(config)# system
ruckus(config-sys)# interface
ruckus(config-sys-if)# ip name-server 192.168.0.1
The command was executed successfully.
```

ip addr

To set the controller's IP address and netmask, use the following command:

```
ip addr <IP-ADDR> <NET-MASK>
```

Use a space to separate the IP address and netmask.

Syntax Description

ip addr	Configure the controller's IP address and netmask
<IP-ADDR>	Set the controller's IP address to this value
<NET-MASK>	Set the controller's netmask to this value

Defaults

None.

Example

```
ruckus# config
ruckus(config)# system
ruckus(config-sys)# interface
ruckus(config-sys-if)# ip addr 192.168.0.1 255.255.255.0
The command was executed successfully.
```

ip mode

To set the controller's IP address mode, use the following command:

```
ip mode <dhcp|static>
```

Syntax Description

`ip mode`	Configure the controller's IP address mode
`dhcp`	Set the controller's IP address mode to DHCP
`static`	Set the controller's IP address mode to static

Defaults

None.

Example

To set the controller's IP address mode to DHCP, enter the following command:

```
ruckus# config
ruckus(config)# system
ruckus(config-sys)# interface
ruckus(config-sys-if)# ip mode dhcp
The command was executed successfully.
```

show

To display the current management interface settings, use the following command:

```
show
```

Syntax Description

`show`	Display the current management interface settings

Defaults

None.

Example

```
ruckus# config
ruckus(config)# system
ruckus(config-sys)# interface
ruckus(config-sys-if)# show
Protocol Mode= IPv4-Only
Device IP Address:
Mode= Manual
IP Address= 192.168.11.100
Netmask= 255.255.255.0
Gateway Address= 192.168.11.1
Primary DNS= 192.168.11.1
Secondary DNS= 168.95.1.1

Management VLAN:
Status= Disabled
```

```
VLAN ID=

ruckus(config-sys-if)#
```

ipv6 enable

To enable IPv6 addressing, use the following command:

```
ipv6 enable
```

ipv6 route gateway

To set the controller's IPv6 gateway addressing, use the following command:

```
ipv6 route gateway <GATEWAY-ADDR>
```

ipv6 name-server

To set the IPv6 DNS server, use the following command:

```
name-server <DNS-ADDR> [<DNS-ADDR>]
```

ipv6 addr

To set the IPv6 addressing, use the following command:

```
addr <IPv6-ADDR> <IPv6-PREFIX>
```

ipv6 mode

To set the IPv6 address mode, use the following command:

```
ipv6 mode [auto|manual]
```

vlan

To enable the management VLAN and set the VLAN ID, use the following command:

```
vlan <NUMBER>
```

no ip

To disable IPv4 addressing, use the following command:

```
no ip
```

no ipv6

To disable IPv6 addressing, use the following command:

```
no ipv6
```

no ntp

To disable the NTP client, use the following command:

```
no ntp
```

Syntax Description

`no ntp`	Disable the NTP client on the controller.

Defaults

Enabled. The default NTP server addresss is `ntp.ruckuswireless.com`.

Example

```
ruckus(config-sys)# no ntp
The NTP settings have been updated.
```

ntp

To enable the NTP client, use the following command:

```
ntp <IP-ADDR/DOMAIN-NAME>
```

Syntax Description

`ntp`	Enable the NTP client
`<IP-ADDR/DOMAIN-NAME>`	Set the NTP server address to this IP address/domain name

Defaults

None.

Example

```
ruckus(config-sys)# ntp 192.168.2.21
The NTP settings have been updated.
ruckus(config-sys)# ntp sohu.com
The NTP settings have been updated.
```

ftp-anon

To enable FTP anonymous access, use the following command:

```
ftp-anon
```

no ftp-anon

To disable FTP anonymouse access, use the following command:

```
no ftp-anon
```

ftp

Enable FTP server.

no ftp

Disable FTP server.

kt-hotspot

To set KT hotspot authentication message encrypt key, use the following command:

```
kt-hotspot <ENCRYPT-KEY> [<LOGOUT-URL>] [<AUTH-PORT>] [<IP-ADDR>]
```

Syntax Description

`kt-hotspot`	Enable KT hotspot. Use a space ( ) to separate the logout URL, authentication port and receive authentication message public IP address if ZD set up internal network. It will take effect after system reboot.
`ENCRYPT-KEY`	Set the KT hotspot encryption key
`LOGOUT-URL`	Set the KT hotspot logout URL
`AUTH-PORT`	Set the KT hotspot authentication port
`IP-ADDR`	Set the KT hotspot public IP address

Defaults

None.

Example

```
ruckus(config-sys)# kt-hotspot key123 logout.url.com 223 192.0.11.100
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-sys)#
```

no kt-hotspot

Disables KT web authentication. Takes effect after system reboot.

Smart Redundancy Commands

To configure the Smart Redundancy settings, you must first enter the `config-sys-smart-redundancy` context from within the config-sys context.

smart-redundancy

To enter the config-sys-smart-redundancy context and configure Smart Redundancy settings, use the following command:

```
smart-redundancy
```

Example

```
ruckus# config
```

```
ruckus(config)# system
ruckus(config-sys)# smart-redundancy
ruckus(config-sys-smart-redundancy)#
```

no smart-redundancy

Disables the smart redundancy settings.

peer-addr

To configure the Smart Redundancy peer IP address, use the following command

```
peer-addr <IP-ADDR>
```

secret

To configure the Smart Redundancy shared secret, use the following command:

```
secret <WORD>
```

show

To displays information about smart redundancy, use the following command:

```
show
```

Management Interface Commands

To configure management interface settings, you must first enter the config-sys-mgmt-if context from the config-sys context.

mgmt-if

To enter the `config-sys-mgmt-if` context and configure the management interface settings, use the following command:

```
mgmt-if
```

Syntax Description

`mgmt-if`	Configure the management interface settings

Defaults

None.

Example

```
ruckus(config-sys)# mgmt-if
ruckus(config-sys-mgmt-if)#
```

no mgmt-if

To disable the management interface, use the following command:

```
no mgmt-if
```

Syntax Description

`no mgmt-if`	Disable the management interface

Defaults

None.

Example

```
ruckus(config-sys)# no mgmt-if
    The management interface has been updated.
```

ip addr

To set the management interface IP address, use the following command:

```
ip addr <IP-ADDR> <NET-MASK>
```

gateway

To set the management interface gateway address, use the following command:

```
gateway <GATEWAY-ADDR>
```

no gateway

To disable the management interface gateway address, use the following command:

```
no gateway
```

vlan

To enable the management VLAN and set the VLAN ID, use the following command:

```
vlan <NUMBER>
```

mgmt-if-ipv6

To enter the `config-sys-mgmt-if-ipv6` context and configure the management interface settings, use the following command:

```
mgmt-if-ipv6
```

Syntax Description

`mgmt-if-ipv6`	Configure the management interface settings

Defaults

None.

Example

```
ruckus(config-sys)# mgmt-if-ipv6
ruckus(config-sys-mgmt-if-ipv6)#
```

no mgmt-if-ipv6

To disable the management interface, use the following command:

```
no mgmt-if-ipv6
```

Syntax Description

`no mgmt-if-ipv6`	Disable the management interface

Defaults

None.

Example

```
ruckus(config-sys)# no mgmt-if-ipv6
    The management interface has been updated.
```

ipv6 addr

To set the management interface IP address, use the following command:

```
ip addr <IPv6-ADDR> <IPv6-PREFIX>
```

gateway

To set the management interface gateway address, use the following command:

```
gateway <GATEWAY-ADDR>
```

no gateway

To disable the management interface gateway address, use the following command:

```
no gateway
```

vlan

To enable the management VLAN and set the VLAN ID, use the following command:

```
vlan <NUMBER>
```

flexmaster

To set the FlexMaster server address and the periodic inform interval, use the following command:

```
flexmaster <IP-ADDR/DOMAIN-NAME> interval <NUMBER>
```

Syntax Description

`flexmaster`	Configure the FlexMaster server settings

`<IP-ADDR/DOMAIN-NAME>`	Set to this URL or IP address
`interval`	Configure the periodic inform interval
`<NUMBER>`	Set to this interval (in minutes)

Defaults None.

Example

```
ruckus(config-sys)# flexmaster http://172.18.30.118 interval 30
The FlexMaster Management settings have been updated.
```

no flexmaster

To disable FlexMaster management of the controller, use the following command:

```
no flexmaster
```

Syntax Description

`no flexmaster`	Disable FlexMaster management of the controller

Defaults None

Example

```
ruckus(config-sys)# no flexmaster
FlexMaster Management has been disabled.
```

northbound

To enable northbound portal interface support and set the northbound portal password, use the following command:

```
northbound password <WORD>
```

Defaults Disabled

Example

```
ruckus(config-sys)# northbound password pass123
The northbound portal interface settings have been updated.
```

no northbound

To disable northbound portal interface support, use the following command:

```
no northbound
```

Example

```
ruckus(config-sys)# no northbound
Northbound portal interface has been disabled.
```

SNMPv2 Commands

Use the following commands to configure SNMPv2 settings. To use these commands, you must first enter the config-sys-snmpv2 context.

snmpv2

To configure the SNMPv2 settings, use the following command:

```
snmpv2
```

Executing this command enters the `config-sys-snmpv2` context.

Syntax Description

`snmpv2`	Configure the SNMPv2 settings

Example

```
ruckus(config-sys)# snmpv2
ruckus(config-sys-snmpv2)#
```

contact

To enable SNMPv2 agent and set the system contact, use the following command:

```
contact <WORD>
```

location

To enable SNMPv2 agent and set the system location, use the following command:

```
location <WORD>
```

ro-community

To set the read-only (RO) community name, use the following command:

```
ro-community <WORD>
```

Syntax Description

ro-community	Configure the read-only community name
<WORD>	Set the read-only community name to this value

Defaults

public

Example

```
ruckus(config-sys-snmpv2)# ro-community private-123
The command was executed successfully
```

rw-community

To set the read-write (RW) community name, use the following command:

```
rw-community <WORD>
```

This command must be entered from within the `snmp-agent` context.

Syntax Description

rw-community	Configure the read-write community name
<WORD>	Set the read-write community name to this value

Defaults

private

Example

```
ruckus(config-sys-snmpv2)# rw-community private-123
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

show

To display SNMPv2 agent and SNMP trap settings, use the show command.

SNMPv3 Commands

Use the following commands to configure SNMPv3 settings. To use these commands, you must first enter the config-sys-snmpv3 context.

snmpv3

To configure the SNMPv3 settings, use the following command:

```
snmpv3
```

Executing this command enters the `config-sys-snmpv3` context.

Syntax Description

`snmpv3`	Configure the SNMPv3 settings

Defaults

```
ruckus(config-sys)# snmpv3
ruckus(config-sys-snmpv3)#
```

ro-user

To set the SNMPv3 Read Only User, use the following command:

```
ro-user <WORD> [MD5|SHA] <WORD> [DES|AES|NONE] <WORD>
```

rw-user

To set the SNMPv3 Read Write User, use the following command:

```
rw-user <WORD> [MD5|SHA] <WORD> [DES|AES|NONE] <WORD>
```

snmp-trap-format

To set the SNMP trap format to SNMPV2 or SNMPV3, use the following command:

```
snmp-trap-format [SNMPv2 | SNMPv3]
```

Syntax Description

`snmp-trap-format`	Set the SNMP trap format
`[SNMPv2 | SNMPv3]`	Set to either SNMPv2 or SNMPv3

Defaults

SNMPv2

Example

```
ruckus(config-sys)# snmp-trap-format SNMPV2
The SNMP trap settings have been updated.
```

snmpv2-trap

To enable the SNMPv2 trap and set the IP address of the trap server, use the following command:

```
snmpv2-trap <NUMBER> <IP/IPv6-ADDR>
```

Syntax Description

`snmpv2-trap`	Enable the SNMPv2 trap and set the trap server's IP address
`<NUMBER>`	Assign the trap receiver ID (1-4)
`<IP/IPv6-ADDR>`	Set the trap receiver IP address

Defaults

None

Example

```
ruckus(config-sys)# snmpv2-trap 1 192.168.10.22
The SNMP trap settings have been updated.
```

snmpv3-trap

To enable and configure the SNMPv3 trap parameters, use the following command:

```
snmpv3-trap <user_name> <snmp_trap_server_ip> [MD5 | SHA]
<auth_pass_phrase> [DES <privacy_phrase>|AES <privacy_phrase>|
None]
```

Syntax Description

`snmpv3-trap`	Enable the SNMPv3 trap and configure the trap parameters
`<user_name>`	Trap user name
`<snmp_trap_server_ip>`	Trap server IP address

[MD5 | SHA]	Authentication method
<auth_pass_phrase>	Authentication passphrase
[DES <privacy_phrase>| AES <privacy_phrase>| None]	Privacy method and privacy phrase

Defaults None

Example
```
ruckus(config-sys)#snmpv3-trap test1234 192.168.0.22 MD5
test1234 DES test4321
The command was executed successfully.
```

no snmp-trap-ap

To disable SNMP trap server configuration for AP, use the following command:

```
no snmp-trap-ap
```

Example
```
ruckus(config-sys)#no snmp-trap-ap
The SNMP AP trap settings have been updated.
```

Syslog Settings Commands

Use the `syslog` commands to configure the controller's syslog notification settings. To run these commands, you must first enter the `config-sys` context.

no syslog

To disable syslog notification, use the following command:

```
no syslog
```

Syntax Description

no syslog	Disable syslog notification

Defaults Disabled.

Example
```
ruckus# config
```

```
ruckus(config)# system
ruckus(config-sys)# no syslog
The command was executed successfully.
```

syslog

To enable syslog notifications and enter the config-sys-syslog context, use the following command:

```
syslog
```

server

To set the syslog server address, use the following command:

```
server <IP-ADDR>
```

Syntax Description

`server`	Set the syslog server IP address.
<IPADDR>	Send syslog notifications to this IP address.

Defaults

Disabled.

facility

To set the facility name, use the following command:

```
facility <FACILITY NAME>
```

Syntax Description

`facility` <FACILITY NAME>	Sets the syslog facility name (local0 - local7)

Defaults

Disabled.

priority

To set the syslog priority level, use the following command:

```
priority <PRIORITY LEVEL>
```

Syntax Description

`priority` <PRIORITY LEVEL>	Sets the syslog priority level (emerg, alert, crit, err, warning, notice, info, debug).

Defaults

Disabled.

ap-facility

To set the AP syslog facility name, use the following command:

```
ap-facility <FACILITY-NAME>
```

Syntax Description

`ap-facility <FACILITY-NAME>`	Sets the AP syslog facility name (local0 - local7).

Defaults

Disabled.

ap-priority

To set the AP syslog priority level, use the following command:

```
ap-priority <PRIORITY LEVEL>
```

Syntax Description

`ap-priority <PRIORITY LEVEL>`	Sets the AP syslog priority level (emerg, alert, crit, err, warning, notice, info, debug).
<IPADDR>	Send syslog notifications to this IP address.

Defaults

Disabled.

Example

```
ruckus# config
ruckus(config)# system
ruckus(config-sys)# syslog
ruckus(config-sys-syslog)# server 192.168.3.10
The syslog settings have been updated.
ruckus(config-sys-syslog)# facility local0
The syslog settings have been updated.
ruckus(config-sys-syslog)# priority emerg
The syslog settings have been updated.
ruckus(config-sys-syslog)# ap-facility local0
The syslog settings have been updated.
ruckus(config-sys-syslog)# ap-priority emerg
The syslog settings have been updated.
ruckus(config-sys-syslog)# end
The syslog settings have been updated.
Your changes have been saved.
ruckus(config-sys)#
```

bypasscna

Use the following command to bypass Apple Captive Network Assistance (CNA) on iDevices and OS X machines.

```
bypasscna <WLAN-TYPE>
```

Syntax Description

bypasscna	Bypass Apple Captive Network Assistance (CNA) on iDevices and OS X machines
<WLAN-TYPE>	Enter the WLAN service type (web-auth, guestaccess, wispr)

Example

```
ruckus(config-sys)# bypasscna web-auth
```

no bypasscna

To disable the ignore Apple CNA feature, use the following command:

```
no bypasscna
```

Example

```
ruckus(config-sys)# no bypasscna
```

no syslog-ap

To disable external syslog server configuration for AP, use the following command:

```
no syslog-ap
```

Example

```
ruckus(config-sys)#no syslog-ap
The AP syslog settings have been updated.
```

Management Access Control List Commands

Use the following commands to create or configure management ACLs and enter the config-sys-mgmt-acl or config-sys-mgmt-acl-ipv6 contexts. These commands must be used from the config-sys context.

no mgmt-acl

To delete a management ACL for IPv4, use the following command:

```
no mgmt-acl <WORD>
```

mgmt-acl

To create or configure a management ACL, use the following command:

```
mgmt-acl <WORD>
```

Executing this command enters the `config-mgmt-acl` context.

Syntax Description

`mgmt-acl`	Create or configure a management ACL
`<WORD>`	Create or configure this management ACL

Defaults

None.

Example

```
ruckus(config-sys)# mgmt-acl macl1
The management ACL 'macl1' has been created. To save the Management
ACL, type 'end' or 'exit'.
ruckus(config-mgmt-acl)#
```

no mgmt-acl-ipv6

To delete a management ACL for IPv6, use the following command:

```
no mgmt-acl-ipv6 <WORD>
```

mgmt-acl-ipv6

To create or configure an IPv6 management ACL, use the following command:

```
mgmt-acl-ipv6 <WORD>
```

Executing this command enters the `config-mgmt-acl-ipv6` context.

Syntax Description

`mgmt-acl-ipv6`	Create or configure a management ACL
`<WORD>`	Create or configure this management ACL

Defaults

None.

Example

```
ruckus(config-sys)# mgmt-acl-ipv6 macl1
The management ACL 'macl1' has been created. To save the Management
ACL, type 'end' or 'exit'.
ruckus(config-mgmt-acl-ipv6)#
```

exit

Saves changes, and then exits the config-mgmt-acl context.

end

Saves changes, and then exits the config-mgmt-acl context.

quit

Exits the config-mgmt-acl context without saving changes.

abort

Exits the config-mgmt-acl context without saving changes.

name

To set the management ACL name, use the following command:

```
name <WORD>
```

restrict-type

To set the management ACL restriction type, use the following command:

```
restrict-type [single ip-addr <IP-ADDR> | range ip-range <IP-
ADDR> <IP-ADDR> | subnet ip-subnet <IP-ADDR> <IP-SUBNET>]
```

Syntax Description

`restrict-type`	Set the management ACL restriction type (single/range)
`single ip-addr`	Set management ACL restriction type to single
`range`	Sets the management ACL restriction type to range.
`ip-range`	Sets the IP address range for management ACL. Use a space ( ) to separate addresses.
`subnet ip-subnet`	Sets the subnet for management acl IP address. Use a space ( ) to separate IP address and Netmask (128.0.0.0 to 255.255.255.252).

show

To display management ACL settings, use the show command.

QoS Commands

Use the following commands to configure QoS settings on the controller. These commands must be executed from the config-sys context.

no qos

To disable QoS on the controller, use the following command:

```
no qos
```

Syntax Description

`no qos`	Disable QoS on the controller

Defaults

None.

Example

```
ruckus(config-sys)# no qos
Changes are saved!
System QoS function has been disabled.
```

qos

To enable and configure Quality of Service settings on the controller, use the following command:

```
qos
```

Executing this command enters the `config-sys-qos` context. The following commands can be executed from within the qos context.

Example

```
ruckus(config-sys)# qos
ruckus(config-sys-qos)#
```

heuristics video inter-packet-gap

Use the following command to set the QoS heuristics video inter-packet gap minimum/maximum values:

```
heuristics video inter-packet-gap min <NUMBER> max <NUMBER>
```

heuristics video packet-length

Use the following command to set the heuristics video packet-length values:

```
heuristics video packet-length min <NUMBER> max <NUMBER>
```

heuristics voice inter-packet-gap

Use the following command to set the heuristics voice inter-packet-gap values:

```
heuristics voice inter-packet-gap min <NUMBER> max <NUMBER>
```

heuristics voice packet-length

Use the following command to set the heuristics voice packet-length values:

```
heuristics voice packet-length min <NUMBER> max <NUMBER>
```

heuristics classification video packet-octet-count

Use the following command to set the heuristics classification video packet-octet-count value:

```
heuristics classification video packet-octet-count <NUMBER>
```

heuristics classification voice packet-octet-count

Use the following command to set the heuristics classification voice packet-octect-count value:

```
heuristics classification voice packet-octet-count <NUMBER>
```

heuristics no-classification video packet-octet-count

Use the following command to set the heuristics no-classification video packet-octet-count value

```
heuristics no-classification video packet-octet-count <NUMBER>
```

heuristics no-classification voice packet-octet-count

Use the following command to set the heuristics no-classification voice packet-octet-count value

```
heuristics no-classification voice packet-octet-count <NUMBER>
```

tos classification video

Use the following command to set the TOS classification video value:

```
tos classification video <WORD>
```

tos classification voice

Use the following command to set the TOS classification voice value:

```
tos classification voice <WORD>
```

tos classification data

Use the following command to set the TOS classification data value:

```
tos classification data <WORD>
```

tos classification background

Use the following command to set the TOS classification background value:

```
tos classification background <WORD>
```

show

Use the following command to display the system QoS settings:

```
show
```

tunnel-mtu

To set the tunnel MTU, use the following command:

```
tunnel-mtu <NUMBER>
```

Syntax Description

`tunnel-mtu`	Set the tunnel MTU

Defaults

None.

Example

```
ruckus(config-sys)# tunnel-mtu 1500
The Tunnel MTU settings have been updated.
ruckus(config-sys)#
```

bonjour

To enable bonjour service, use the following command:

```
bonjour
```

Defaults

Disabled.

Example

```
ruckus(config-sys)# bonjour
The bonjour service settings have been updated.
ruckus(config-sys)#
```

no bonjour

To disable bonjour service, use the following command:

```
no bonjour
```

telnetd

To enable the telnet server, use the following command:

```
telnetd
```

Syntax Description

`telnetd`	Enable the telnet server

Defaults None.

Example

```
ruckus(config-sys)# telnetd
The telnet server settings have been updated.
ruckus(config-sys)#
```

no telnetd

To disable the telnet server, use the following command:

```
telnetd
```

Syntax Description

`no telnetd`	Disable the telnet server

Defaults None.

Example

```
ruckus(config-sys)# no telnetd
The telnet server settings have been updated.
ruckus(config-sys)#
```

static-route

To create and configure static route settings, use the following command:

```
static-route <WORD>
```

Syntax Description

`static-route`	Create and configure a static route
`name <WORD>`	Set the name of the static route
`subnet <IP-SUBNET>`	Set the subnet for the destination network. Use a slash (/) to separate IP address and subnet
`gateway <GATEWAY-ADDR>`	Set the gateway address
`show`	Show a list of all static routes

Defaults None.

Example

```
ruckus(config-sys)# static-route route1
The static route 'route1' has been created. To save the static
route, type 'end' or 'exit'.
ruckus(config-static-route)# subnet 192.168.11.1/24
```

```
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-static-route)# gateway 192.168.11.1
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-static-route)# show
Static Route:
ID=
Name= route1
IP subnet= 192.168.11.1/24
IP gateway= 192.168.11.1

ruckus(config-static-route)#
```

no static-route

To delete a static route, use the following command:

```
no static-route
```

static-route-ipv6

To create and configure IPv6 static route settings, use the following command:

```
static-route-ipv6 <WORD>
```

Syntax Description

`static-route-ipv6`	Create and configure a static route
`name <WORD>`	Set the name of the static route
`prefix <IPv6-PREFIX>`	Set the subnet for the destination network. Use a slash (/) to separate IP address and prefix length
`gateway <GATEWAY-ADDR>`	Set the gateway address
`show`	Show a list of all static routes

Defaults

None.

Example

```
ruckus(config-sys)# static-route route1
The static route 'route1' has been created. To save the static
route, type 'end' or 'exit'.
ruckus(config-static-route)# subnet 192.168.11.1/24
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

```
ruckus(config-static-route)# gateway 192.168.11.1
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-static-route)# show
Static Route:
ID=
Name= route1
IP subnet= 192.168.11.1/24
IP gateway= 192.168.11.1

ruckus(config-static-route)#
```

no static-route-ipv6

To delete an IPv6 static route, use the following command:

```
no static-route-ipv6 <WORD>
```

show

Use the following command to display system configuration information:

```
show
```

support-entitle

Use the following command to manually download entitlement file:

```
support-entitle
```

no snmpv2

To disable the SNMPv2 agent, use the following command:

```
no snmpv2
```

Syntax Description

`no snmpv2`	Disables the SNMPv3 agent

Defaults

None.

Example

```
ruckus(config-sys)# no snmpv2
The SNMP v2 agent settings have been updated.
```

no snmpv3

To disable the SNMPv3 agent, use the following command:

```
no snmpv3
```

Syntax Description

`no snmpv3`	Disables the SNMPv3 agent

Defaults

None.

Example

```
ruckus(config-sys)# no snmpv3
The SNMP v3 agent settings have been updated.
```

no snmp-trap

To disable the SNMP trap notifications, use the following command:

```
no snmp-trap <NUMBER>
```

Syntax Description

`no snmp-trap`	Disables SNMP trap notification by index

Defaults

None.

Example

```
ruckus(config-sys)# no snmp-trap 1
The SNMP trap settings have been updated.
```

no snmpv2-trap

To disable the SNMP trap notifications, use the following command:

```
no snmp-trap <NUMBER>
```

Syntax Description

`no snmpv2-trap`	Disables SNMP trap notification by index

Defaults

None.

Example

```
ruckus(config-sys)# no snmpv2-trap 1
The SNMP trap settings have been updated.
```

no snmpv3-trap

To disable the SNMPv3 trap notification, use the following command:

```
no snmpv3-trap <NUMBER>
```

Syntax Description

`no snmpv3-trap`	Disables SNMP trap notification by index

Defaults

None.

Example

```
ruckus(config-sys)# no snmpv3-trap 1
The SNMP trap settings have been updated.
```

snmp-trap

To set the SNMP trap format, use the following command:

```
snmp-trap {trap server address}
```

Syntax Description

`snmp-trap`	Enable SNMP trap notifications
{trap server address}	Set the trap server address to this IP address or host name

Defaults

None.

Example

```
ruckus# config
ruckus(config)# system
ruckus(config-sys)# snmp-trap 192.168.0.3
```

Management ACL Commands

Use the `mgmt-acl` commands to configure the management ACL settings. To run these commands, you must first enter the `config-mgmt-acl` context.

abort

To exit the `config-mgmt-acl` context without saving changes, use the abort command.

```
abort
```

Syntax Description

`abort`	Exit the context without saving changes

Defaults

Disabled.

Example

```
ruckus(config-mgmt-acl)# abort
No changes have been saved.
ruckus(config-sys)#
```

end

To save changes, and then exit the config-services context, use the following command:

```
end
```

Syntax Description

`end`	Save changes, and then exit the context

Defaults

Disabled.

Example

```
ruckus(config-mgmt-acl)# end
The management ACL 'macl2' has been updated and saved.
Your changes have been saved.
ruckus(config-sys)#
```

exit

To save changes, and then exit the config-services context, use the following command:

```
exit
```

Syntax Description

`exit`	Save changes, and then exit the context

Defaults

Disabled.

Example

```
ruckus(config-mgmt-acl)# exit
The management ACL 'macl2' has been updated and saved.
Your changes have been saved.
ruckus(config-sys)#
```

quit

To exit the `config-mgmt-acl` context without saving changes, use the abort command.

```
quit
```

Syntax Description

`quit`	Exit the context without saving changes

Defaults

Disabled.

Example

```
ruckus(config-mgmt-acl)# quit
No changes have been saved.
ruckus(config-sys)#
```

name

To set the management ACL name, use the following command:

```
name <WORD>
```

Syntax Description

`name`	Set the management ACL name
`<WORD>`	Set to this name

Defaults

Disabled.

Example

```
ruckus(config-mgmt-acl)# name macl2
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

restrict-type single ip-addr

To set the management ACL restriction type to a single IP address, use the following command:

```
restrict-type single ip-addr <ip_address>
```

Syntax Description

`restrict-type single ip-addr`	Set the management ACL restriction type to a single IP address
`<ip_address>`	Set to this IP address only

Defaults

Disabled.

Example

```
ruckus(config-mgmt-acl)# restrict-type single ip-addr
192.168.110.22
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

restrict-type subnet ip-subnet

To set the management ACL restriction type to certain subnets, use the following command:

```
restrict-type subnet ip-subnet <IP-SUBNET> <IP-SUBNET>
```

Syntax Description

`restrict-type subnet ip-subnet`	Set the management ACL restriction type to a single IP address
`<IP-SUBNET>`	Set to this subnet

Defaults

Disabled.

Example

```
ruckus(config-mgmt-acl)#restrict-type subnet ip-subnet
172.30.110.26 255.255.254.0
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

restrict-type range ip-range

To set the management ACL restriction type to an IP address range, use the following command:

```
restrict-type range ip-range <ip_address> <ip_address>
```

Syntax Description

`restrict-type range ip-range`	Set the management ACL restriction type to a single IP address
`<ip_address> <ip_address>`	Set to this IP address range. The first `<ip_address>` is for the startui

Defaults

Disabled.

Example

```
ruckus(config-mgmt-acl)#restrict-type range ip-range
172.30.110.28 172.30.110.39
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

show

To display the current management ACL settings, use the following command:

```
show
```

Syntax Description

`show`	Display the current management ACL settings

Defaults

Disabled.

Example

```
ruckus(config-mgmt-acl)# show
Management ACL:
ID:
:
Name= macl2
Restriction Type= range
IP range= 172.30.110.28-172.30.110.39
```

Configure UPNP Settings

Use the following commands to enable or disable Universal Plug and Play:

upnp

```
upnp
```

Syntax Description

upnp	Enable UPnP

Defaults

None.

Example

```
ruckus(config)# upnp
UPnP Service is enabled
/bin/upnp enable
ruckus(config)#
```

no upnp

```
no upnp
```

Syntax Description

no upnp	Enable UPnP

Defaults

None.

Example

```
ruckus(config)# no upnp
UPnP Service is disabled
/bin/upnp disable
ruckus(config)#
```

Configure Zero-IT Settings

To configure Zero-IT settings, use the following commands.

zero-it

To configure Zero-IT settings, use the following command:

```
zero-it [local | name <WORD>]
```

zero-it-auth-server

To configure Zero-IT settings, use the following command:

```
zero-it-auth-server [local | name <WORD>]
```

Syntax Description

zero-it	Set Zero-IT authentication server
zero-it-auth-server	Set Zero-IT authentication server
local	Set the Zero-IT authentication server to local database
name	Set the Zero-IT authentication server to an external AAA server
<WORD>	Name of AAA server

Defaults

None.

Example

```
ruckus(config)# zero-it-auth-server name radius
The Authentication Server of Zero IT Activation has been updated.
ruckus(config)#
```

Example

```
ruckus(config)# zero-it-auth-server local
The Authentication Server of Zero IT Activation has been updated.
ruckus(config)#
zero-it-auth-server
```

Configure Dynamic PSK Expiration

The following section lists commands for configuring Dynamic Pre-Shared Keys.

dynamic-psk-expiration

To set DPSK expiration, use the following command:

```
dynamic-psk-expiration <TIME>
```

Syntax Description

`dynamic-psk-expiration`	Set DPSK expiration
`<TIME>`	Set DPSK expiration to this time limit (one-day, one-week, two-weeks, one-month, two-months, three-months, half-a-year, one-year, two-years)
unlimited	Set DPSKs to never expire

Defaults

None.

Example

```
ruckus(config)# dynamic-psk-expiration unlimited
The Dynamic psk expiration value has been updated.
ruckus(config)#
```

Configure WLAN Settings Commands

Use the `config-wlan` commands to configure the WLAN settings, including the WLAN's description, SSID, and its security settings. To run these commands, you must first enter the `config-wlan` context.

wlan

To create a WLAN or configure an existing WLAN, use the following command:

```
wlan <WORD/NAME>
```

Executing this command enters the config-wlan context.

Syntax Description

wlan	Configure a WLAN
<WORD/NAME>	Name of the WLAN service

Defaults

None.

Example

```
ruckus(config)# wlan ruckus2
The WLAN service 'ruckus2' has been created. To save the WLAN
service, type 'end' or 'exit'.
ruckus(config-wlan)#
```

abort

Exits the config-wlan context without saving changes.

end

Saves changes, and then exits the config-wlan context.

exit

Saves changes, and then exits the config-wlan context.

quit

Exits the config-wlan context without saving changes.

description

To set the WLAN service description, use the following command:

```
description <WORD>
```

Syntax Description

description	Configure the WLAN description
<WORD>	Set the WLAN description this value

Defaults

None.

Example

```
ruckus(config-wlan)# description ruckustestwlan2
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-wlan)#
```

called-station-id-type

To set the called station ID type to, use the following command:

```
called-station-id-type [wlan-bssid | ap-mac]
```

Syntax Description

wlan-bssid	Set the called station ID type to 'BSSID:SSID'
ap-mac	Set the called station ID type to 'APMAC:SSID'

Defaults

wlan-bssid

Example

```
ruckus(config-wlan)# called-station-id-type wlan-bssid
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

ssid

To set the WLAN service's SSID or network name, use the following command:

```
ssid <SSID>
```

Syntax Description

ssid	Configure the WLAN service's SSID
<SSID>	Set the SSID to this value

Defaults

None.

Example

```
ruckus(config-wlan)# ssid ruckus2
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-wlan)#
```

beacon-interval

To set the beacon interval for mesh links, use the following command:

```
beacon-interval <NUMBER>
```

Syntax Description

beacon-interval	Set the beacon interval for the WLAN
<NUMBER>	Enter the beacon interval (100~1000 TUs)

Defaults

100

Example

```
ruckus(config-wlan)# beacon-interval 100
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-wlan)#
```

mgmt-tx-rate

To set the transmit rate for management frames, use the following command:

```
mgmt-tx-rate <RATE>
```

Syntax Description

mgmt-tx-rate	Set the max transmit rate for management frames
<RATE>	Set the transmit rate (in Mbps).

Defaults

2

Example

```
ruckus(config-wlan)# mgmt-tx-rate 2
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-wlan)#
```

name

To set the name of the WLAN, use the following command:

```
name <NAME>
```

Syntax Description

name	Set the WLAN name
<NAME>	Set to this name

Defaults

None.

Example

```
ruckus(config-wlan)# name ruckus2
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-wlan)#
```

type

To configure the WLAN type, use the following command:

```
type [standard-usage | guest-access | hotspot <WORD> | hs20
<WORD>]
```

Syntax Description

type	Set the WLAN type
standard-usage	Set the WLAN type to standard usage
guest-access	Set the WLAN type to guest access
hotspot <WORD>	Set the WLAN type to Hotspot using the hotspot service specified
hs20 <WORD>	Set the WLAN type to Hotspot 2.0 using the HS2.0 operator specified

Defaults None.

Example

```
ruckus(config-wlan)# type standard-usage
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-wlan)#
```

open none

To set the authentication method to 'open' and encryption method to 'none', use the following command:

```
open none
```

Syntax Description

open	Set the authentication method to 'open'
none	Set the encryption method to 'none'

Defaults None.

Example

```
ruckus(config)# wlan randy-wlansvc-01-open
The WLAN service 'randy-wlansvc-01-open' has been created. To save
the WLAN service, type end or exit.
ruckus(config-wlan-randy-wlansvc-01-open)# open none
The command was executed successfully.
ruckus(config-wlan-randy-wlansvc-01-open)#
```

open wpa passphrase algorithm AES

To set the authentication method to 'open', encryption method to 'WPA', and algorithm to 'AES', use the following command:

```
open wpa passphrase <PASSPHRASE> algorithm AES
```

Syntax Description

open	Set the authentication method to open
wpa	Set the encryption method to WPA
passphrase <PASSPHRASE>	Set the WPA passphrase to <PASSPHRASE>
algorithm AES	Set the encryption algorithm to AES

Defaults None.

Example

```
ruckus(config)# wlan randy-wlansvc-01-open
The WLAN service 'randy-wlansvc-01-open' has been created. To save
the WLAN service, type end or exit.
ruckus(config-wlan-randy-wlansvc-01-open)# open wpa passphrase
12345678 algorithm AES
The command was executed successfully.
ruckus(config-wlan-randy-wlansvc-01-open)#
```

open wpa passphrase algorithm TKIP

To set the authentication method to 'open', encryption method to 'WPA', and algorithm to 'TKIP', use the following command:

```
open wpa passphrase <PASSPHRASE> algorithm TKIP
```

Syntax Description

open	Set the authentication method to open
wpa	Set the encryption method to WPA
passphrase <PASSPHRASE>	Set the WPA passphrase to <PASSPHRASE>
algorithm TKIP	Set the encryption algorithm to TKIP

Defaults

None.

Example

```
ruckus(config)# wlan randy-wlansvc-01-open
The WLAN service 'randy-wlansvc-01-open' has been created. To save
the WLAN service, type end or exit.
ruckus(config-wlan-randy-wlansvc-01-open)# open wpa passphrase
12345678 algorithm TKIP
The command was executed successfully.
ruckus(config-wlan-randy-wlansvc-01-open)#
```

open wpa passphrase algorithm auto

To set the authentication method to 'open', encryption method to 'WPA', and algorithm to 'Auto', use the following command:

```
open wpa passphrase <PASSPHRASE> algorithm auto
```

Syntax Description

open	Set the authentication method to open
wpa	Set the encryption method to WPA

passphrase <PASSPHRASE>	Set the WPA passphrase to <PASSPHRASE>
algorithm auto	Set the encryption algorithm to Auto

Defaults

None.

Example

```
ruckus(config)# wlan randy-wlansvc-01-open
The WLAN service 'randy-wlansvc-01-open' has been created. To save
the WLAN service, type end or exit.
ruckus(config-wlan-randy-wlansvc-01-open)# open wpa passphrase
12345678 algorithm auto
The command was executed successfully.
ruckus(config-wlan-randy-wlansvc-01-open)#
```

open wpa2 passphrase algorithm AES

To set the authentication method to 'open', encryption method to 'WPA2', and algorithm to 'AES', use the following command:

```
open wpa2 passphrase <PASSPHRASE> algorithm AES
```

Syntax Description

open	Set the authentication method to open
wpa2	Set the encryption method to WPA2
passphrase <PASSPHRASE>	Set the WPA2 passphrase to <PASSPHRASE>
algorithm AES	Set the encryption algorithm to AES

Defaults

None.

Example

```
ruckus(config)# wlan randy-wlansvc-01-open
The WLAN service 'randy-wlansvc-01-open' has been created. To save
the WLAN service, type end or exit.
ruckus(config-wlan-randy-wlansvc-01-open)# open wpa2 passphrase
12345678 algorithm AES
The command was executed successfully.
ruckus(config-wlan-randy-wlansvc-01-open)#
```

open wpa2 passphrase algorithm TKIP

To set the authentication method to 'open', encryption method to 'WPA2', and algorithm to 'TKIP', use the following command:

```
open wpa2 passphrase <PASSPHRASE> algorithm TKIP
```

Syntax Description

open	Set the authentication method to open
wpa2	Set the encryption method to WPA2
passphrase <PASSPHRASE>	Set the WPA2 passphrase to <PASSPHRASE>
algorithm TKIP	Set the encryption algorithm to TKIP

Defaults

None.

Example

```
ruckus(config)# wlan randy-wlansvc-01-open
The WLAN service 'randy-wlansvc-01-open' has been created. To save
the WLAN service, type end or exit.
ruckus(config-wlan-randy-wlansvc-01-open)# open wpa2 passphrase
12345678 algorithm TKIP
The command was executed successfully.
ruckus(config-wlan-randy-wlansvc-01-open)#
```

open wpa2 passphrase algorithm auto

To set the authentication method to 'open', encryption method to 'WPA2', and algorithm to 'Auto', use the following command:

```
open wpa2 passphrase <PASSPHRASE> algorithm auto
```

Syntax Description

open	Set the authentication method to open
wpa2	Set the encryption method to WPA2
passphrase <PASSPHRASE>	Set the WPA passphrase to <PASSPHRASE>
algorithm auto	Set the encryption algorithm to Auto

Defaults

None.

Example

```
ruckus(config)# wlan randy-wlansvc-01-open
The WLAN service 'randy-wlansvc-01-open' has been created. To save
the WLAN service, type end or exit.
ruckus(config-wlan-randy-wlansvc-01-open)# open wpa2 passphrase
12345678 algorithm auto
The command was executed successfully.
ruckus(config-wlan-randy-wlansvc-01-open)#
```

open wpa-mixed passphrase algorithm auto

To set the authentication method to 'open', encryption method to 'WPA mixed', and algorithm to 'Auto', use the following command:

```
open wpa-mixed passphrase <PASSPHRASE> algorithm [AES | TKIP | auto]
```

Syntax Description

open	Set the authentication method to open
wpa-mixed	Set the encryption method to WPA-mixed
passphrase <PASSPHRASE>	Set the WPA passphrase to <PASSPHRASE>
algorithm AES	Set the encryption algorithm to AES
algorithm TKIP	Set the encryption algorithm to TKIP
algorithm auto	Set the encryption algorithm to Auto

Defaults

None.

Example

```
ruckus(config-wlan)# open wpa-mixed passphrase pass1234 algo-
rithm auto
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-wlan)#
```

open wep-64 key {KEY} key-id {KEY-ID}

To set the authentication method to 'open', encryption method to 'WEP-64', key index, and WEP key, use the following command:

```
open wep-64 key {key} key-id {key ID}
```

Syntax Description

open	Set the authentication method to open
wep-64	Set the encryption method to WEP 64-bit
key {key}	Set the WEP key to {key}
key-id {key ID}	Set the WEP key ID to {key ID}

Defaults

None.

Example

```
ruckus(config)# wlan randy-wlansvc-01-open
The WLAN service 'randy-wlansvc-01-open' has been created. To save
the WLAN service, type end or exit.
```

```
ruckus(config-wlan-randy-wlansvc-01-open)# open wep-64 key
1234567890 key-id 1
The command was executed successfully.
ruckus(config-wlan-randy-wlansvc-01-open)#
```

open wep-128 key key-id

To set the authentication method to 'open', encryption method to 'WEP-128', key index, and WEP key, use the following command:

```
open wep-128 key {key} key-id {key ID}
```

Syntax Description

open	Set the authentication method to open
wep-128	Set the encryption method to WEP 128-bit
key {key}	Set the WEP key to {key}
key-id {key ID}	Set the WEP key ID to {key ID}

Defaults

None.

Example

```
ruckus(config)# wlan randy-wlansvc-01-open
The WLAN service 'randy-wlansvc-01-open' has been created. To save
the WLAN service, type end or exit.
ruckus(config-wlan-randy-wlansvc-01-open)# open wep-128 key
12345678901234567890123456 key-id 1
The command was executed successfully.
ruckus(config-wlan-randy-wlansvc-01-open)#
```

mac none auth-server

To set the authentication method to 'MAC Address' and encryption method to 'none', use the following command:

```
mac none auth-server <WORD>
```

Syntax Description

mac	Set the authentication method to 'MAC Address'
none	Set the encryption method to 'none'
auth-server <WORD>	Set the authorization server address to <WORD>

Defaults

None.

Example

```
ruckus(config-wlan-randall-wlansvc-01)# mac none auth-server
Ruckus-Auth-01
```

```
The command was executed successfully.
ruckus(config-wlan-randall-wlansvc-01)#
```

mac wpa passphrase alogrithm AES auth-server

To set the authentication method to 'MAC Address', encryption method to 'WPA', and algorithm to 'AES', use the following command:

```
mac wpa passphrase <PASSPHRASE> algorithm AES auth-server <WORD>
```

Syntax Description

mac	Set the authentication method to 'MAC Address'
wpa	Set the encryption method to 'WPA'
passphrase <PASSPHRASE>	Set the WPA passphrase to <PASSPHRASE>
algorithm AES	Set the encryption algorithm to 'AES'
auth-server <WORD>	Set the authorization server address to <WORD>

Defaults

None.

Example

```
ruckus(config-wlan-randall-wlansvc-01)# mac wpa passphrase
12345678 algorithm AES auth-server Ruckus-Auth-01
The command was executed successfully.
ruckus(config-wlan-randall-wlansvc-01)#
```

mac wpa passphrase alogrithm TKIP auth-server

To set the authentication method to 'MAC Address', encryption method to 'WPA', and algorithm to 'TKIP', use the following command:

```
mac wpa passphrase <PASSPHRASE> alogrithm TKIP auth-server
<WORD>
```

Syntax Description

mac wpa	Set the authentication method to 'MAC Address' and encryption method to 'WPA'
passphrase <PASSPHRASE>	Set the WPA passphrase to <PASSPHRASE>
algorithm TKIP	Set the encryption algorithm to 'TKIP'
auth-server <WORD>	Set the authorization server address to <WORD>

Defaults

None.

Example

```
ruckus(config-wlan-randall-wlansvc-01)# mac wpa passphrase
12345678 algorithm TKIP auth-server Ruckus-Auth-01
The command was executed successfully.
ruckus(config-wlan-randall-wlansvc-01)#
```

mac wpa2 passphrase alogrithm AES auth-server

To set the authentication method to 'MAC Address', encryption method to 'WPA2', and algorithm to 'AES', use the following command:

```
mac wpa2 passphrase <PASSPHRASE> alogrithm AES auth-server
<WORD>
```

Syntax Description

mac wpa2	Set the authentication method to 'MAC Address' and encryption method to 'WPA2'
passphrase <PASSPHRASE>	Set the WPA2 passphrase to <PASSPHRASE>
algorithm AES	Set the encryption algorithm to 'AES'
auth-server <WORD>	Set the authorization server address to <WORD>

Defaults

None.

Example

```
ruckus(config-wlan-randall-wlansvc-01)# mac wpa2 passphrase
12345678 algorithm AES auth-server Ruckus-Auth-01
The command was executed successfully.
ruckus(config-wlan-randall-wlansvc-01)#
```

mac wpa2 passphrase alogrithm TKIP auth-server

To set the authentication method to 'MAC Address', encryption method to 'WPA2', and algorithm to 'TKIP', use the following command:

```
mac wpa2 passphrase <PASSPHRASE> alogithm TKIP auth-server
<WORD>
```

Syntax Description

mac wpa2	Set the authentication method to 'MAC Address' and encryption method to 'WPA2'
passphrase <PASSPHRASE>	Set the WPA2 passphrase to <PASSPHRASE>
algorithm TKIP	Set the encryption algorithm to 'TKIP'
auth-server <WORD>	Set the authorization server address to <WORD>

Defaults

None.

Example

```
ruckus(config-wlan-randall-wlansvc-01)# mac wpa2 passphrase
12345678 algorithm TKIP auth-server Ruckus-Auth-01
The command was executed successfully.
ruckus(config-wlan-randall-wlansvc-01)#
```

mac wpa-mixed passphrase algorithm AES auth-server

To set the authentication method to 'MAC Address', encryption method to WPA-Mixed, and algorithm to AES, use the following command:

```
mac wpa-mixed passphrase <PASSPHRASE> algorithm AES auth-server
<WORD>
```

Syntax Description

`mac wpa-mixed`	Set the authentication method to 'MAC Address' and encryption method to 'WPA-Mixed'
`passphrase <PASSPHRASE>`	Set the WPA2 passphrase to <PASSPHRASE>
`algorithm AES`	Set the encryption algorithm to 'AES'
`auth-server <WORD>`	Set the authorization server to this auth server

Defaults

None.

Example

```
ruckus(config-wlan)# mac wpa-mixed passphrase pass1234 algorithm
AES auth-server radius
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-wlan)#
```

mac wpa-mixed passphrase algorithm TKIP auth-server

To set the authentication method to 'MAC Address', encryption method to 'WPA-Mixed', algorithm to TKIP, use the following command:

```
mac wpa-mixed passphrase <PASSPHRASE> algorithm TKIP auth-server
<WORD>
```

Syntax Description

`mac wpa-mixed`	Set the authentication method to 'MAC Address' and encryption method to 'WPA-Mixed'
`passphrase <PASSPHRASE>`	Set the WPA2 passphrase to <PASSPHRASE>
`algorithm TKIP`	Set the encryption algorithm to 'TKIP'
`auth-server <WORD>`	Set the authorization server to this auth server

Defaults

None.

Example

```
ruckus(config-wlan)# mac wpa-mixed passphrase pass1234 algorithm
TKIP auth-server radius
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-wlan)#
```

mac wep-64 key key-id auth-server

To set the authentication method to 'MAC Address', encryption method to 'WEP-64', key index, and WEP key, use the following command:

```
mac wep-64 key {KEY} key-id {KEY-ID} auth-server <WORD>
```

Syntax Description

`mac`	Set the authentication method to MAC address
`wep-64`	Set the encryption method to WEP 64-bit
`key {KEY}`	Set the WEP key to {KEY}
`key-id {KEY-ID}`	Set the WEP key ID to {KEY-ID}
`auth-server <WORD>`	Set the authorization server address to <WORD>

Defaults

None.

Example

```
ruckus(config-wlan-randy-wlansvc-01-wpa2)# mac wep-64 key
15791BD8F2 key-id 2 auth-server Ruckus-Auth-01
The command was executed successfully.
ruckus(config-wlan-randy-wlansvc-01-wpa2)#
```

mac wep-128 key key-id auth-server

To set the authentication method to 'MAC Address', encryption method to 'WEP-128', key index, and WEP key, use the following command:

```
mac wep-128 key {KEY} key-id {KEY-ID} auth-server <WORD>
```

Syntax Description

`mac`	Set the authentication method to MAC address
`wep-128`	Set the encryption method to WEP 128-bit
`key {KEY}`	Set the WEP key to {key}
`key-id {KEY-ID}`	Set the WEP key ID to {key ID}
`auth-server <WORD>`	Set the authorization server address to <WORD>

Defaults

None.

Example

```
ruckus(config-wlan-randy-wlansvc-01-wpa2)# mac wep-128 key
15715791BD8F212345691BD8F2 key-id 2 auth-server Ruckus-Auth-01
The command was executed successfully.
ruckus(config-wlan-randy-wlansvc-01-wpa2)#
```

shared wep-64

To set the authentication method to 'Shared', encryption method to 'WEP-64', key index, and WEP key, use the following command:

```
shared wep-64 key {KEY} key-id {KEY-ID}
```

Syntax Description

`shared`	Set the authentication method to 'Shared'
`wep-64`	Set the encryption method to WEP 64-bit
`key {KEY}`	Set the WEP key to {key}
`key-id {KEY-ID}`	Set the WEP key ID to {KEY-ID}

Defaults

None.

Example

```
ruckus(config-wlan-randy-wlansvc-01-wpa2)# shared authentication
encryption wep-64 key 15791BD8F2 key-id 2
The command was executed successfully.
ruckus(config-wlan-randy-wlansvc-01-wpa2)#
```

shared wep-128 key key-id

To set the authentication method to 'Shared', encryption method to 'WEP-128', key index, and WEP key, use the following command:

```
shared wep-128 key {KEY} key-id {KEY-ID}
```

Syntax Description

`shared`	Set the authentication method to 'Shared'
`wep-128`	Set the encryption method to WEP 128-bit
`key {KEY}`	Set the WEP key to {key}
`key-id {KEY-ID}`	Set the WEP key ID to {KEY-ID}

Defaults

None.

Example

```
ruckus(config-wlan-randy-wlansvc-01-wpa2)# shared wep-128 key
15791B15791BD8F2123456D8F2 key-id 2
The command was executed successfully.
ruckus(config-wlan-randy-wlansvc-01-wpa2)#
```

dot1x eap-type EAP-SIM auth-server

To set the authentication method to 'EAP-SIM', use the following command:

```
dot1x eap-type EAP-SIM auth-server[local | name <WORD>]
```

Syntax Description

`dot1x`	Set the authentication method to '802.11x'
`eap-type`	Set the EAP type
`EAP-SIM`	Set the authentication method to EAP-SIM
`auth-server`	Set authentication server
`local`	Set the authentication server to 'local database'
`name`	Set the auth server
`<WORD>`	Name of the auth server

Defaults

None.

Example

```
ruckus(config-wlan)# dot1x eap-type EAP-SIM auth-server local
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

dot1x eap-type PEAP auth-server

To set the authentication method to 'PEAP', use the following command:

```
dot1x eap-type PEAP auth-server [local | name <WORD>]
```

Syntax Description

`dot1x`	Set the authentication method to ‘802.11x’
`eap-type`	Set the EAP type
`PEAP`	Set the authentication method to PEAP
`auth-server`	Set authentication server
`local`	Set the authentication server to ‘local database’
`name`	Set the auth server
`<WORD>`	Name of the auth server

Defaults

`None.`

Example

```
ruckus(config-wlan)# dot1x eap-type PEAP auth-server local
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

dot1x wpa algorithm AES auth-server

To set the authentication method to '802.1x EAP', encryption method to 'WPA', and algorithm to 'AES', use the following command:

```
dot1x wpa algorithm AES auth-server [local | name <WORD>]
```

Syntax Description

`dot1x`	Set the authentication method to ‘802.11x’
`wpa`	Set the encryption method to WPA
`algorithm AES`	Set the algorithm to AES
`auth-server`	Set authentication server
`local`	Set the authentication server to ‘local database’
`name`	Set the auth server
`<WORD>`	Name of the auth server

Defaults

None.

Example

```
ruckus(config-wlan-wlansvc-012)# dot1x wpa algorithm AES auth-
server Ruckus-Auth-01
The command was executed successfully.
ruckus(config-wlan-wlansvc-012)#
```

dot1x wpa algorithm TKIP auth-server

To set the authentication method to '802.1x EAP', encryption method to 'WPA', and algorithm to 'TKIP', use the following command:

```
dot1x wpa algorithm TKIP auth-server <WORD>
```

Syntax Description

`dot1x`	Set the authentication method to '802.11x'
`wpa`	Set the encryption method to WPA
`algorithm TKIP`	Set the algorithm to TKIP
`auth-server`	Set authentication server
`local`	Set the authentication server to 'local database'
`name`	Set the auth server
`<WORD>`	Name of the auth server

Defaults

None.

Example

```
ruckus(config-wlan-wlansvc-012)# dot1x wpa algorithm TKIP auth-server Ruckus-Auth-01
The command was executed successfully.
```

dot1x wpa algorithm auto auth-server

To set the authentication method to '802.1x EAP', encryption method to 'WPA', and algorithm to 'Auto', use the following command:

```
dot1x wpa algorithm auto auth-server [local | name <WORD>]
```

Syntax Description

`dot1x`	Set the authentication method to '802.11x'
`wpa`	Set the encryption method to WPA
`algorithm auto`	Set the algorithm to Auto
`auth-server`	Set authentication server
`local`	Set the authentication server to 'local database'
`name`	Set the auth server
`<WORD>`	Name of the auth server

Defaults

None.

Example

```
ruckus(config-wlan-wlansvc-012)# dot1x wpa algorithm auto auth-server Ruckus-Auth-01
```

```
The command was executed successfully.
ruckus(config-wlan-wlansvc-012)#
```

dot1x wpa2 algorithm AES auth-server

To set the authentication method to '802.1x EAP', encryption method to 'WPA2', and algorithm to 'AES', use the following command:

```
dot1x wpa2 algorithm AES auth-server [local | name <WORD>]
```

Syntax Description

`dot1x`	Set the authentication method to ’802.11x’
`wpa2`	Set the encryption method to WPA2
`algorithm AES`	Set the algorithm to AES
`auth-server`	Set authentication server
`local`	Set the authentication server to ‘local database’
`name`	Set the auth server
`<WORD>`	Name of the auth server

Defaults

None.

Example

```
ruckus(config-wlan-randy-wlansvc-01-open)# dot1x wpa2 algorithm
AES auth-server Ruckus-RADIUS
The command was executed successfully.
ruckus(config-wlan-wlansvc-01-open)#
```

dot1x wpa2 algorithm TKIP auth-server

To set the authentication method to '802.1x EAP', encryption method to 'WPA2', and algorithm to 'TKIP', use the following command:

```
dot1x wpa2 algorithm TKIP auth-server [local | name <WORD>]
```

Syntax Description

`dot1x`	Set the authentication method to ’802.11x’
`wpa2`	Set the encryption method to WPA2
`algorithm TKIP`	Set the algorithm to TKIP
`auth-server`	Set authentication server
`local`	Set the authentication server to ‘local database’
`name`	Set the auth server
`<WORD>`	Name of the auth server

Defaults

None.

Example

```
ruckus(config-wlan-wlansvc-012)# dot1x authentication encryption
wpa2 algorithm TKIP auth-server Ruckus-Auth-01
The command was executed successfully.
ruckus(config-wlan-wlansvc-012)#
```

dot1x wpa2 algorithm auto auth-server

To set the authentication method to '802.1x EAP', encryption method to 'WPA2', and algorithm to 'Auto', use the following command:

```
dot1x wpa2 algorithm auto auth-server [local | name <WORD>]
```

Syntax Description

`dot1x`	Set the authentication method to '802.11x'
`wpa2`	Set the encryption method to WPA2
`algorithm auto`	Set the algorithm to auto
`auth-server`	Set authentication server
`local`	Set the authentication server to 'local database'
`name`	Set the auth server
`<WORD>`	Name of the auth server

Defaults

None.

Example

```
ruckus(config-wlan-wlansvc-012)# dot1x wpa2 algorithm auto auth-
server Ruckus-Auth-01
The command was executed successfully.
ruckus(config-wlan-wlansvc-012)#
```

dot1x wpa-mixed algorithm AES auth-server

To set the authentication method to 802.1x EAP, encryption method to WPA-Mixed, and encryption method to AES, use the following command:

```
dot1x wpa-mixed algorithm AES auth-server [local | name <WORD>]
```

Syntax Description

`dot1x`	Set the authentication method to '802.11x'
`wpa-mixed`	Set the encryption method to WPA-Mixed
`algorithm AES`	Set the algorithm to AES

auth-server	Set authentication server
local	Set the authentication server to 'local database'
name	Set the auth server
<WORD>	Name of the auth server

Defaults

None.

Example

```
ruckus(config-wlan-wlansvc-012)# dot1x wpa-mixed algorithm AES
auth-server local
The command was executed successfully.
ruckus(config-wlan-wlansvc-012)#
```

dot1x wpa-mixed algorithm TKIP auth-server

To set the authentication method to 802.1x EAP, encryption method to WPA-Mixed, and encryption method to TKIP, use the following command:

```
dot1x wpa-mixed algorithm TKIP auth-server [local | name <WORD>]
```

Syntax Description

dot1x	Set the authentication method to '802.11x'

wpa-mixed	Set the encryption method to WPA-Mixed
algorithm TKIP	Set the algorithm to TKIP
local	Set the authentication server to 'local database'
name	Set the auth server
<WORD>	Name of the auth server

Defaults

None.

Example

```
ruckus(config-wlan-wlansvc-012)# dot1x wpa-mixed algorithm AES
auth-server local
The command was executed successfully.
ruckus(config-wlan-wlansvc-012)#
```

dot1x wpa-mixed algorithm auto auth-server

To set the authentication method to 802.1x EAP, encryption method to WPA-Mixed, and encryption method to Auto, use the following command:

```
dot1x wpa-mixed algorithm auto auth-server [local | name <WORD>]
```

Syntax Description

`dot1x`	Set the authentication method to ‘802.11x’
`wpa-mixed`	Set the encryption method to WPA-Mixed
`algorithm auto`	Set the algorithm to Auto
`local`	Set the authentication server to ‘local database’
`name`	Set the auth server
`<WORD>`	Name of the auth server

Defaults

None.

Example

```
ruckus(config-wlan-wlansvc-012)# dot1x wpa-mixed algorithm AES
auth-server local
The command was executed successfully.
ruckus(config-wlan-wlansvc-012)#
```

dot1x authentication encryption wep-64 auth-server

To set the authentication method to '802.1x EAP', encryption method to 'WEP-64', key index, and WEP key, use the following command:

```
dot1x authentication encryption wep-64 auth-server {auth server}
```

Syntax Description

dot1x authentication	Set the authentication method to ‘802.11x’
encryption wep-64	Set the encryption method to WEP 64-bit
`auth-server {auth server}`	Set the auth server to `{auth server}`

Defaults

None.

Example

```
ruckus(config-wlan-wlansvc-012)# dot1x authentication encryption
wep-64 auth-server Ruckus-Auth-01
The command was executed successfully.
ruckus(config-wlan-wlansvc-012)#
```

dot1x wep-128 auth-server

To set the authentication method to '802.1x EAP', encryption method to 'WEP-128', key index, and WEP key, use the following command:

```
dot1x wep-128 auth-server [local|name <WORD>]
```

Syntax Description

dot1x	Set the authentication method to '802.11x'
wep-128	Set the encryption method to WEP 128-bit
`auth-server [local|name<WORD>]`	Set the auth server to local or to the named server

Defaults

None.

Example

```
ruckus(config-wlan-wlansvc-012)# dot1x authentication encryption wep-128 auth-server Ruckus-Auth-01
The command was executed successfully.
ruckus(config-wlan-wlansvc-012)#
```

dot1x none

To set the encryption as none and authentication server to 'Local Database' or the named server, use the following command:

```
dot1x none auth-server [local|name<WORD>]
```

Syntax Description

dot1x none	Set the authentication method to '802.1x' and encryption to none
`auth-server [local|name<WORD>]`	Set the auth server to local or to the named server

Defaults

None.

Example

```
ruckus(config-wlan-wlansvc-012)# dot1x none auth-server Ruckus-Auth-01
The command was executed successfully.
ruckus(config-wlan-wlansvc-012)#
```

dot1x-mac none

To set the encryption as none and authentication method to 802.1x-MAC, use the following command:

```
dot1x-mac none auth-server name <WORD>
```

Syntax Description

dot1x-mac none	Set the authentication method to '802.1x-MAC' and encryption to none
`auth-server name<WORD>`	Set the auth server to the named server

Defaults None.

Example

```
ruckus(config-wlan-wlansvc-012)# dot1x-mac none auth-server
Ruckus-Auth-01
The command was executed successfully.
ruckus(config-wlan-wlansvc-012)#
```

bgscan

To enable background scanning on the WLAN, use the following command:

```
bgscan
```

Example

```
ruckus(config-wlan)# bgscan
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-wlan)#
```

no bgscan

To disable background scanning on the WLAN, use the following command:

```
no bgscan
```

Example

```
ruckus(config-wlan)# no bgscan
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-wlan)#
```

client-isolation

To enable client isolation, use the following command:

```
client-isolation [local|full]
```

Syntax Description

`client-isolation`	Enable client isolation for this WLAN
`local`	Wireless clients associated with the same AP will be unable to communicate with one another locally.
`full`	Wireless clients will be unable to communicate with each other or access any of the restricted subnets.

Example

```
ruckus(config-wlan)# client-isolation local
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

```
ruckus(config-wlan)#
```

no client-isolation

To enable client isolation, use the following command:

```
no client-isolation
```

Syntax Description

`no client-isolation`	Disable client isolation for this WLAN

Example

```
ruckus(config-wlan)# no client-isolation
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-wlan)#
```

load-balancing

To enable load balancing for this WLAN, use the following command:

```
load-balancing
```

Example

```
ruckus(config-wlan)# load-balancing
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-wlan)#
```

no load-balancing

To disable load balancing for this WLAN, use the following command:

```
no load-balancing
```

Example

```
ruckus(config-wlan)# no load-balancing
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-wlan)#
```

send-eap-failure

To enable send EAP failure messages, use the following command:

```
send-eap-failure
```

Example

```
ruckus(config-wlan)# send-eap-failure
```

```
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-wlan)#
```

no send-eap-failure

To disable send EAP failure messages, use the following command:

```
no send-eap-failure
```

Example

```
ruckus(config-wlan)# no send-eap-failure
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-wlan)#
```

pap-authenticator

To enable RADIUS message authenticator in PAP requests, use the following command:

```
pap-authenticator
```

Example

```
ruckus(config-wlan)# pap-authenticator
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-wlan)#
```

no pap-authenticator

To disable RADIUS message authenticator in PAP requests, use the following command:

```
no pap-authenticator
```

Example

```
ruckus(config-wlan)# no pap-authenticator
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-wlan)#
```

nasid-type

To set the NAS ID type, use the following command:

```
nasid-type [wlan-bssid|mac-addr|user-define <WORD>]
```

Syntax Description

`nasid-type`	Set the NAS ID type
`wlan-bssid`	Set NAS ID type WLAN-BSSID (default)
`mac-addr`	Set NAS ID type to Controller MAC Address
`user-define <WORD>`	Set NAD ID type to a user-defined string

Default

wlan-bssid

Example

```
ruckus(config-wlan)# nasid-type wlan-bssid
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-wlan)#
```

priority low

To set the WLAN priority to low, use the following command:

```
priority low
```

priority high

To set the WLAN priority to high, use the following command:

```
priority high
```

web-auth

To enable Web authentication, use the following command:

```
web-auth [local | name <WORD>]
```

Syntax Description

web-auth	Enable Web authentication
local	Use local database as auth server
name	Specify an external auth server
<WORD>	The AAA server to use for Web authentication

Defaults

None.

Example

```
ruckus# config
ruckus(config)# wlan wlan-123
ruckus(config-wlan-wlan-123)# web-auth Ruckus-RADIUS
The command was executed successfully.
ruckus(config-wlan-wlan-123)#
```

no web-auth

To disable Web authentication, use the following command:

```
no web-auth
```

Syntax Description

no web-auth	Disable Web authentication

Defaults

None.

Example

```
ruckus# config
ruckus(config)# wlan wlan-123
ruckus(config-wlan-wlan-123)# no web-auth
The command was executed successfully.
```

grace-period

To set the grace period (idle timeout), use the following command:

```
grace-period <NUMBER>
```

Syntax Description

grace-period	Enables and Sets a maximum time (in minutes) for which users must re-authenticate after disconnecting.

Defaults

Disabled.

Example

```
ruckus(config-wlan)# grace-period 20
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

no grace-period

To disable the grace period (idle timeout), use the following command:

```
no grace-period <NUMBER>
```

Syntax Description

no grace-period	Disables grace period timeout.

Defaults

Disabled.

Example

```
ruckus(config-wlan)# no grace-period
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

acct-server

To set the accounting server, use the following command:

```
acct-server <WORD>
```

Syntax Description

acct-server	Configure the AAA server
<WORD>	Set the AAA server to this address

Defaults

None.

Example

```
ruckus# config
ruckus(config)# wlan wlan-123
ruckus(config-wlan-wlan-123)# acct-server Ruckus-Acct-01
The command was executed successfully.
```

acct-server interim-update

To configure the interim update frequency (in minutes) of the AAA server, use the following command:

```
acct-server <WORD> interim-update <NUMBER>
```

Syntax Description

acct-server	Confgure the interim update frequency of the AAA server
interim-update{minutes}	Set the update frequency to this value (in minutes)

Defaults

5 (minutes)

Example

```
ruckus# config
ruckus(config)# wlan wlan-123
ruckus(config-wlan-wlan-123)# acct-server Ruckus-Acct-01
interim-update 5
The command was executed successfully.
```

no acct-server

To disable the AAA server, use the following command:

```
no acct-server
```

Syntax Description

no acct-server	Disable AAA server authentication

Defaults

None.

Example

```
ruckus# config
ruckus(config)# wlan wlan-123
ruckus(config-wlan-wlan-123)# no acct-server
The command was executed successfully.
```

inactivity-timeout

To enable and set the inactivity timeout, use the following command:

```
inactivity-timeout <NUMBER>
```

Syntax Description

inactivity-timeout	Enable and set the inactivity timeout
<NUMBER>	Set the inactivity timeout in minutes

Defaults

5

Example

```
ruckus(config-wlan)# inactivity-timeout 15
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-wlan)#
```

vlan

To enable the VLAN and set the VLAN ID, use the following command:

```
vlan <NUMBER>
```

Syntax Description

vlan	Enable VLAN
<NUMBER>	Set the VLAN ID to this value

Defaults

None.

Example

```
ruckus# config
ruckus(config)# wlan wlan-123
ruckus(config-wlan-wlan-123)# vlan 12
The command was executed successfully.
```

dynamic-vlan

To enable dynamic VLAN, use the following command:

```
dynamic-vlan
```

Syntax Description

dynamic-vlan	Enable dynamic VLAN

Notes

Dynamic VLAN can be enabled or disabled in the following two conditions: 1) The authentication method is '802.1X/EAP' or 'MAC Address', Encryption method is WPA, WPA2, WPA mixed, or none. 2) Authentication method is 'Open', Encryption method is WPA, WPA2 (Algorithm may not be Auto), enable Zero-IT Activation, enable Dynamic PSK.

Example

```
ruckus(config-wlan)# dynamic-vlan
The command was executed successfully. To save the changes, type
'end' or 'exit'
```

no dynamic-vlan

To disable dynamic VLAN, use the following command:

```
no dynamic-vlan
```

Syntax Description

no dynamic-vlan	Disable dynamic VLAN

Defaults

Disabled.

Example

```
ruckus(config-wlan)# no dynamic-vlan
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

mcast-filter

To enable multicast filter for the WLAN, use the following command:

```
mcast-filter
```

no mcast-filter

To disable multicast filter for the WLAN, use the following command:

```
no mcast-filter
```

hide-ssid

To hide an SSID from wireless users, use the following command.Wireless users who know the SSID will still be able to connect to the WLAN service.

```
hide-ssid
```

Syntax Description

hide-ssid	Hide SSID from wireless users

Defaults

None.

Example

```
ruckus# config
ruckus(config)# wlan wlan-123
ruckus(config-wlan-wlan-123)# hide-ssid
The command was executed successfully.
```

no hide-ssid

To unhide or broadcast an SSID to wireless users, use the following command:

```
no hide-ssid
```

Syntax Description

no hide-ssid	Broadcast SSID to wireless users

Defaults

None.

Example

```
ruckus# config
ruckus(config)# wlan wlan-123
ruckus(config-wlan-wlan-123)# no hide-ssid
The command was executed successfully
```

ofdm-only

To enable support of OFDM rates only, use the following command:

```
ofdm-only
```

no ofdm-only

To disable OFDM only rates, use the following command:

```
no ofdm-only
```

admission-control

To enable Call Admission Control, use the following command:

```
admission-control
```

no admission-control

To disable Call Admissino Control, use the following command:

```
no admission-control
```

bss-minrate

To set the minimum BSS transmission rate of the WLAN (in Mbps), use the following command:

```
bss-minrate <NUMBER>
```

Syntax Description

bss-minrate	Set the minimum BSS transmission rate in Mbps.
<NUMBER>	Minimum BSS transmission rate

Defaults

None.

Example

```
ruckus(config-wlan)# bss-minrate 2
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-wlan)#
```

no bss-minrate

To disable the minimum BSS transmission rate for the WLAN, use the following command:

```
no bss-minrate
```

tunnel-mode

To enable tunnel mode, use the following command:

```
tunnel-mode
```

Syntax Description

tunnel-mode	Enable tunnel mode

Defaults

None.

Example

```
ruckus# config
ruckus(config)# wlan wlan-123
ruckus(config-wlan-wlan-123)# tunnel-mode
The command was executed successfully.
```

no tunnel-mode

To disable the tunnel mode, use the following command:

```
no tunnel-mode
```

Syntax Description

no tunnel-mode	Disable the tunnel mode

Defaults

None.

Example

```
ruckus# config
ruckus(config)# wlan wlan-123
ruckus(config-wlan-wlan-123)# no tunnel-mode
The command was executed successfully.
```

dhcp-relay

To set the DHCP relay server to the specified address (tunneled WLANs only), use the following command:

```
dhcp-relay <WORD>
```

no dhcp-relay

To disable DHCP relay, use the following command:

```
no dhcp-relay
```

option82

To enable DHCP option82, use the following command:

```
option82
```

no option82

To disable DHCP option 82, use the following command:

```
no option82
```

sta-info-extraction

To enable station information extraction (client fingerprinting), use the following command:

```
sta-info-extraction
```

no sta-info-extraction

To disable station information extraction (client fingerprinting), use the following command:

```
no sta-info-extraction
```

max-clients

To set the maximum number of clients for a specific WLAN, use the following command:

```
max-clients <NUMBER>
```

Syntax Description

max-clients	Configure the maximum number of clients that the WLAN can support
<NUMBER>	Set the maximum clients to this value

Defaults

None.

Example

To set the maximum number of clients on WLAN-123 to 50, enter this command:

```
ruckus# config
ruckus(config)# wlan wlan-123
ruckus(config-wlan-wlan-123)# max-clients 50
The command was executed successfully.
```

802dot11d

To enable 802.11d for the WLAN, use the following command:

```
802dot11d
```

no 802dot11d

To disable 802.11d for the WLAN, use the following command:

```
no 802dot11d
```

auto-proxy

To enable auto-proxy and set the location of the wpad.dat file, use the following command:

```
auto-proxy [<wpad-saved-on-zd | wpad-saved-on-external-server>]
url <WORD>
```

Syntax Description

auto-proxy	Enable auto-proxy and specify the location of the wpad.dat file
wpad-saved-on-ZD	WPAD.DAT file is saved on ZoneDirector
wpad-saved-on-external-server	WPAD.DAT file is saved on an external server
url	Specify the WPAD URL configured on DHCP/DNS server
<WORD>	Auto-proxy path and file name

Defaults

None.

Example

```
ruckus(config-wlan)# auto-proxy wpad-saved-on-zd url
192.168.0.2/wpad.dat
The file has been loaded into ZoneDirector successfully,Please use
'import' to apply it
ruckus(config-wlan)#
```

no auto-proxy

To disable auto-proxy, use the following command:

```
no auto-proxy
```

import

To import the wpad.dat file into ZoneDirector, use the following command:

```
import
```

pmk-cache

To set the PMK cache time to the specified number in minutes (1~720 minutes), use the following command:

```
pmk-cache timeout <NUMBER>
```

Defaults

720 minutes

no pmk-cache

To disable PMK cache, use the following command:

```
no pmk-cache
```

pmk-cache-for-reconnect

To apply PMK cache when client reconnects (default), use the following command:

```
pmk-cache-for-reconnect
```

no pmk-cache-for-reconnect

To disable application of PMK caching when client reconnects, use the following command:

```
no pmk-cache-for-reconnect
```

When "no pmk-cache-for-reconnect" is set, the controller attempts to look up PMK cache for roaming clients only, so every client reconnection requires a full reauthentication. A graceful roaming (disconnect before connecting to the roam-to AP) is not regarded as roaming from the controller's perspective.

Defaults

Enabled

roaming-acct-interim-update

To enable accounting interim-updates when a client roams, use the following command:

```
roaming-acct-interim-update
```

When "roaming-acct-interim-update" is set, all traffic and session-id data from the original session is carried over to the new session.

Defaults

Disabled.

no roaming-acct-interim-update

To disable accounting interim updates when a client roams (default: disabled), use the following command:

```
no roaming-acct-interim-update
```

zero-it-activation

To enable Zero-IT activation, use the following command:

```
zero-it-activation
zero-it
```

Syntax Description

zero-it-activation	Enable Zero-IT activation
zero-it	Enable Zero-IT activation

Defaults Disabled.

Example

```
ruckus(config-wlan)# zero-it-activation
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

no zero-it-activation

To disable Zero-IT activation, use the following command:

```
no zero-it-activation
no zero-it
```

Syntax Description

no zero-it-activation	Disable Zero-IT activation
no zero-it	Disable Zero-IT activation

Defaults Disabled.

Example

```
ruckus(config-wlan)# no zero-it
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

dynamic-psk enable

To enable Dynamic Pre-Shared Keys, use the following command:

```
dynamic-psk enable
```

Syntax Description

dynamic-psk enable	Enable Dynamic PSK

Defaults None.

Example

```
ruckus(config-wlan)# dynamic-psk enable
The DPSK can't be enabled or disabled when the wlan type is not
Standard Usage and Encryption method is not WPA or WPA2 and
Authentication method is not open and Zero-IT is not enabled.
ruckus(config-wlan)# zero-it
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-wlan)# dynamic-psk enable
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

```
ruckus(config-wlan)#
```

dynamic-psk passphrase-len

To set the Dynamic Pre-Shared Key passphrase length, use the following command:

```
dynamic-psk passphrase-len <NUMBER>
```

no dynamic-psk

To disable Dynamic Pre-Shared Keys on the WLAN, use the following command:

```
no dynamic-psk
```

limit-dpsk

To enable Dynamic PSK limits and set the max number of devices per user, use the following command:

```
limit-dpsk <NUMBER>
```

no limit-dpsk

To disable Dynamic PSK limits, use the following command:

```
no limit-dpsk
```

no l2acl

To disable Layer 2 Access Control Lists, use the following command:

```
no l2acl
```

no l3acl

To disable Layer 3/4 ACLs, use the following command:

```
no l3acl
```

no l3acl-ipv6

To disable Layer 3/4 IPv6 ACLs, use the following command:

```
no l3acl-ipv6
```

no dvcpcy

To disable device policy for this WLAN, use the following command:

```
no dvcpcy
```

rate-limit

To set the rate limiting for the WLAN, use the following command:

```
rate-limit uplink <NUMBER> downlink <NUMBER>
```

Syntax Description

rate-limit	Set the rate limit
uplink	Set the uplink rate limit
downlink	Set the downlink rate limit
<NUMBER>	Set the rate limiting to the value specified. Valid values include 0.10 and between 0.25~20.00 in 0.25 increments.

Defaults

None.

Example

```
ruckus(config-wlan)# rate-limit uplink 20 downlink 20
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-wlan)#
```

no rate-limit

To disable the rate limit, use the following command:

```
no rate-limit
```

Syntax Description

no rate-limit	Disable rate limiting for the WLAN

Defaults

Disabled.

Example

```
ruckus(config-wlan)# no rate-limit
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

mac-auth-8021x-format

To set the MAC auth MAC address format to 802.1X format (00-10-A4-23-19-C0), use the following command:

```
mac-auth-8021x-format
```

Example

```
ruckus(config-wlan)# mac-auth-8021x-format
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-wlan)#
```

no mac-auth-8021x-format

To set the MAC auth MAC address format to default format (0010a42319c0), use the following command:

```
no mac-auth-8021x-format
```

acl

To apply an Access Control List to this WLAN, use the following command:

```
acl [<l2acl>|<l3acl>|<l3acl-ipv6>] <WORD>
```

Syntax Description

acl	Apply a previously saved ACL to this WLAN
l2acl	Apply a Layer 2 ACL
l3acl	Apply a Layer 3/Layer 4/IP ACL
l3acl-ipv6	Apply an IPv6 L3/L4/IP ACL
<WORD>	The name of the ACL

Defaults

None.

Example

```
ruckus(config-wlan)# acl l2acl acl1
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-wlan)#
```

acl dvcpcy

To apply a Device Policy to the WLAN, use the following command:

```
acl dvcpcy <WORD>
```

acl prece

To apply a Precedence Policy to the WLAN, use the following command:

```
acl prece <WORD>
```

qos classification

To enable Quality of Service classification, use the following command:

```
qos classification
```

no qos classification

To disable Quality of Service classification, use the following command:

```
no qos classification
```

qos heuristics-udp

To enable QoS heuristics for UDP traffic, use the following command:

```
qos heuristics-udp
```

no qos heuristics-udp

To disable QoS heuristics for UDP traffic, use the following command:

```
no qos heuristics-udp
```

qos directed-multicast

To enable QoS directed multicast, use the following command:

```
qos directed-multicast
```

no qos directed-multicast

To disable QoS directed multicast, use the following command:

```
no qos directed-multicast
```

qos igmp-snooping

To disable QoS directed multicast, use the following command:

```
qos igmp-snooping
```

no qos igmp-snooping

To disable QoS IGMP snooping, use the following command:

```
no qos igmp-snooping
```

qos mld-snooping

To enable QoS MLD snooping, use the following command:

```
no qos mld-snooping
```

no qos mld-snooping

To disable QoS MLD snooping, use the following command:

```
no qos mld-snooping
```

qos tos-classification

To enable QoS TOS classification, use the following command:

```
qos tos-classification
```

no qos tos-classification

To disable QoS TOS classification, use the following command:

```
no qos tos-classification
```

qos priority high

To set QoS priority to 'high', use the following command:

```
qos priority high
```

qos priority low

To set QoS priority to 'low', use the following command:

```
qos priority low
```

qos directed-threshold

To set the QoS directed threshold, use the following command:

```
qos directed-threshold <NUMBER>
```

disable-dgaf

To disable Downstream Group-Address Frame Forwarding, use the following command (Hotspot 2.0 WLAN only):

```
disable-dgaf
```

no disable-dgaf

To enable Downstream Group-Address Frame Forwarding, use the following command (Hotspot 2.0 WLAN only):

```
no disable-dgaf
```

proxy-arp

To enable Proxy ARP service for the WLAN, use the following command:

```
proxy-arp
```

no proxy-arp

To disable Proxy ARP service for the WLAN, use the following command:

```
no proxy-arp
```

ignor-unauth-stats

To enable ignoring unauthorized client statistics, use the following command:

```
ignor-unauth-stats
```

no ignor-unauth-stats

To disable ignoring unauthorized client statistics, use the following command:

```
no ignor-unauth-stats
```

show

To display the WLAN settings, use the following command:

```
show
```

Syntax Description

show	Display WLAN settings

Defaults

None.

Example

```
ruckus(config)# wlan ruckus1
The WLAN service 'ruckus1' has been loaded. To save the WLAN service,
type 'end' or 'exit'.
ruckus(config-wlan)# show
WLAN Service:
  ID:
    2:
      NAME = ruckus1
      Tx. Rate of Management Frame(2.4GHz) = 2.0Mbps
      Beacon Interval = 100ms
      SSID = ruckus1
      Description =
      Type = Standard Usage
      Authentication = open
      Encryption = none
      Web Authentication = Disabled
      Authentication Server = Disabled
      Accounting Server = Disabled
      Called-Station-Id type = wlan-bssid
      Tunnel Mode = Disabled
      DHCP relay = Disabled
      Background Scanning = Enabled
      Max. Clients = 100
      Client Isolation = None
      Zero-IT Activation = Disabled
      Priority = High
      Load Balancing = Disabled
      Rate Limiting Uplink = Disabled
```

```
        Rate Limiting Downlink = Disabled
        Auto-Proxy configuration:
          Status = Disabled
        Inactivity Timeout:
            Status = Enabled
            Timeout = 5 Minutes
        VLAN-ID = 1
        Dynamic VLAN = Disabled
        Closed System = Disabled
        OFDM-Only State = Disabled
        Multicast Filter State = Disabled
        802.11d State = Disabled
        DHCP Option82 State = Disabled
        Ignore unauthorized client statistic = Disabled
        STA Info Extraction State = Enabled
        BSS Minrate = Disabled
        Call Admission Control State = Disabled
        PMK Cache Timeout= 720 minutes
        PMK Cache for Reconnect= Enabled
        NAS-ID Type= wlan-bssid
        Roaming Acct-Interim-Update= Disabled
        PAP Message Authenticator = Enabled
        Send EAP-Failure = Disabled
        L2/MAC = No ACLS
        L3/L4/IP Address = No ACLS
        L3/L4/IPv6 Address = No ACLS
        Precedence = precedence1
        Proxy ARP = Enabled
        Device Policy = No ACLS

ruckus(config-wlan)#
```

Configure WLAN Group Settings Commands

Use the `wlan-group` commands to configure the settings of a particular WLAN group.

wlan-group

To create a new WLAN group or update an existing WLAN group, use the following command:

```
wlan-group <WORD>
```

Syntax Description

wlan-group	Configure the WLAN group
<WORD>	Name of the WLAN group

Defaults

Default.

Example

```
ruckus# config
ruckus(config)# wlan-group wlangrp-01
The WLAN group has been created. To save the WLAN group, type end
or exit.
```

no wlan-group

To delete a WLAN group from the list, use the following command:

```
no wlan-group <WORD>
```

Syntax Description

no wlan-group	Delete the WLAN group
<WORD>	Name of the WLAN group

Defaults

None.

Example

```
ruckus(config)# no wlan-group wlan-grp-01
The WLAN group 'wlan-grp-01' has been removed.
ruckus(config)#
```

abort

To exit the `wlan-group` context without saving changes, use the `abort` command. Enter this command from within the context of the WLAN group that you are configuring.

```
abort
```

Syntax Description

abort	Exit the WLAN group without saving changes

Defaults

None.

Example

```
ruckus# config
ruckus(config)# wlan-group wlangrp-01
ruckus(config-wlangrp-wlangrp-01)# abort
```

```
No changes have been saved.
```

end

To save changes to the WLAN group settings and exit the `wlan-group` context, use the following command. Enter this command from within the context of the WLAN group that you are configuring.

```
end
```

Syntax Description

`end`	Save changes, and then exit the WLAN group

Defaults

None.

Example

```
ruckus# config
ruckus(config)# wlan-group wlangrp-01
ruckus(config-wlangrp-wlangrp-01)# end
The WLAN group 'hello-wlangrp' has been updated.
Your changes have been saved.
```

exit

To save changes to the WLAN group settings and exit the `wlan-group` context, use the `exit` command. Enter this command from within the context of the WLAN group that you are configuring.

```
exit
```

Syntax Description

`exit`	Save changes, and then exit the WLAN group

Defaults

None.

Example

```
ruckus# config
ruckus(config)# wlan-group wlangrp-01
ruckus(config-wlangrp-wlangrp-01)# exit
The WLAN group 'wlangrp-01' has been updated.
Your changes have been saved.
```

quit

To exit the `wlan-group` context without saving changes, use the following command. Enter this command from within the context of the WLAN group that you are configuring.

```
quit
```

Syntax Description

`quit`	Exit the WLAN group without saving changes

Defaults

None.

Example

```
ruckus# config
ruckus(config)# wlan-group wlangrp-01
ruckus(config-wlangrp-wlangrp-01)# quit
No changes have been saved.
```

name

To set the WLAN group name, use the following command. Enter this command from within the context of the WLAN group that you are configuring.

```
name {WLAN group name}
```

Syntax Description

`name`	Configure the WLAN group name
{WLAN group name}	Set the WLAN group name to this value

Defaults

None.

Example

```
ruckus# config
ruckus(config)# wlan-group wlangrp-01
ruckus(config-wlangrp-wlangrp-01)# name hello-wlangrp
The command was executed successfully.
```

description

To set the WLAN group description, use the following command. Enter this command from within the context of the WLAN group that you are configuring.

```
description {WLAN group description}
```

Syntax Description

`description`	Configure the WLAN group description
{WLAN group description}	Set the WLAN group description to this value

Defaults

None.

Example

```
ruckus# config
ruckus(config)# wlan-group wlangrp-01
ruckus(config-wlangrp-wlangrp-01)# description my-description-123
The command was executed successfully.
```

wlan

To add a WLAN service to the WLAN group, use the following command. Enter this command from within the context of the WLAN group that you are configuring.

```
wlan <WORD>
```

Syntax Description

wlan	Add a WLAN to the WLAN group
<WORD>	Name of the WLAN to be added

Defaults

None.

Example

```
rruckus(config-wlangrp)# wlan ruckus1
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-wlangrp)# show
WLAN Group:
  ID:
    :
      Name= wlangroup1
      Description=
      WLAN Service:
        WLAN1:
          NAME= ruckus1
          VLAN=

ruckus(config-wlangrp)#
```

no wlan

To remove a WLAN service from the WLAN group, use the following command. Enter this command from within the context of the WLAN group that you are configuring.

```
no wlan <WORD>
```

Syntax Description

no wlan	Delete an existing WLAN service from the WLAN group

<WORD>	Name of the WLAN to be removed

Defaults

None.

Example

```
ruckus(config-wlangrp)# no wlan ruckus1
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-wlangrp)#
```

wlan vlan override none

To add a WLAN service to the WLAN group and set the VLAN tag to 'No Change', use the following command. Enter this command from within the context of the WLAN group that you are configuring.

```
wlan <WORD> vlan override none
```

Syntax Description

wlan <WORD>	Add the WLAN to the WLAN group
vlan override none	Set the VLAN tag to No Change

Defaults

None.

Example

```
ruckus(config-wlangrp)# wlan ruckus1 vlan override none
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-wlangrp)#
```

wlan vlan override tag

To add a WLAN service to the WLAN group and set the VLAN tag to the specified VLAN, use the following command:

```
wlan <NAME> vlan override tag <NUMBER>
```

Syntax Description

wlan <NAME>	Add the <NAME> to the WLAN group
vlan override tag <NUMBER>	Set the VLAN tag of <NAME> to the specified <NUMBER>

Defaults

None.

Example

```
ruckus(config-wlangrp)# wlan ruckus1 vlan override tag 12
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-wlangrp)#
```

show

To display WLAN group settings, use the following command:

```
show
```

Defaults

```
ruckus(config-wlangrp)# show
WLAN Group:
  ID:
    1:
      Name= Default
      Description= Default WLANs for Access Points
      WLAN Service:
        WLAN1:
          NAME= Ruckus1
          VLAN=

ruckus(config-wlangrp)#
```

Configure Role Commands

Use the `role` commands to configure user roles on the controller. To run these commands, you must first enter the `config-role` context.

role

To create a new role or modify an existing role, use the following command:

```
role <WORD>
```

Syntax Description

role	Create or modify a user role
<WORD>	Name of role

Defaults

None.

Example

```
ruckus(config)# role role1
The role entry 'role1' has been created
```

```
ruckus(config-role)#
```

no role

To delete a role entry from the list, use the following command:

```
no role <WORD>
```

Syntax Description

no role	Delete a user role
<WORD>	Name of role

Defaults

None.

Example

```
ruckus(config)# no role role1
The Role 'role1' has been deleted.
ruckus(config)#
```

abort

To exit the `config-role` context without saving changes, use the `abort` command. Enter this command from within the context of the role that you are configuring.

```
abort
```

Syntax Description

abort	Exit the role without saving changes

Defaults

None.

Example

```
ruckus(config-role)# abort
No changes have been saved.
ruckus(config)#
```

end

To save changes, and then exit the `config-role` context, use the following command:

```
end
```

Syntax Description

end	Save changes, and then exit the context

Defaults

None.

Example

```
ruckus(config-role)# end
The Role entry has saved successfully.
Your changes have been saved.
ruckus(config)#
```

exit

To save changes, and then exit the `config-role` context, use the following command:

```
exit
```

Syntax Description

exit	Save changes, and then exit the context

Defaults

None.

Example

```
ruckus(config-role)# exit
The Role entry has saved successfully.
Your changes have been saved.
ruckus(config)#
```

quit

To exit the `config-role` context without saving changes, use the `quit` command. Enter this command from within the context of the role that you are configuring.

```
quit
```

Syntax Description

quit	Exit the role without saving changes

Defaults

None.

Example

```
ruckus(config-role)# quit
No changes have been saved.
ruckus(config)#
```

name

To set the name of a user role, use the following command:

```
name <WORD>
```

Syntax Description

name	Set the name of a user role
<WORD>	Set to this role

Defaults None.

Example

```
ruckus(config-role)# name guest33
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

description

To set the description for a user role, use the following command:

```
description <WORD>
```

Syntax Description

description	Set the description of a user role
<WORD>	Set to this description

Defaults None.

Example

```
ruckus(config-role)# description testforCLI
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

group-attributes

To set the group attributes of a user role, use the following command:

```
group-attributes <WORD>
```

Syntax Description

group-attributes	Set the attributes of a user role
<WORD>	Set to this attribute

Defaults None.

Example

```
ruckus(config-role)# group-attributes ruckus1
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

wlan-allowed

To set the WLANs to which a user role will have access, use the following command:

```
wlan-allowed [all | specify-wlan]
```

Syntax Description

wlan-allowed	Set the WLANs to which a role will have access
all	Grant access to all WLANs
specify-wlan	Grant access to a specific WLAN

Defaults

None.

Example

```
ruckus(config-role)# wlan-allowed all
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-role)# wlan-allowed specify-wlan
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

no specify-wlan-access

To remove a particular WLAN from the list of WLANs that a user role can access, use the following command:

```
no specify-wlan-access <WORD/SSID>
```

Syntax Description

no specify-wlan-access	Remove access to a WLAN by a user role
<WORD/SSID>	Remove access to this WLAN

Defaults

None.

Example

```
ruckus(config-role)# no specify-wlan-access joejoe98
The wlan 'joejoe98' has been removed from the Role.
```

specify-wlan-access

To adda particular WLAN to the list of WLANs that a user role can access, use the following command:

```
specify-wlan-access <wlan_ssid>
```

Syntax Description

specify-wlan-access	Add access to a WLAN by a user role
<wlan_ssid>	Add access to this WLAN

Defaults None.

Example

```
ruckus(config-role)# specify-wlan-access joejoe98
The wlan 'joejoe98' has been added to the Role.
```

no guest-pass-generation

To remove guest pass generation privileges from a user role, use the following command:

```
no guest-pass-generation
```

Syntax Description

no guest-pass-generation	Remove guest pass generation privileges from a user role

Defaults None.

Example

```
ruckus(config-role)# no guest-pass-generation
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

guest-pass-generation

To add guest pass generation privileges to a user role, use the following command:

```
guest-pass-generation
```

Syntax Description

guest-pass-generation	Add guest pass generation privileges to a user role

Defaults None.

Example

```
ruckus(config-role)# guest-pass-generation
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

no admin

To remove ZoneDirector administration privileges from a user role, use the following command:

```
no admin
```

Syntax Description

no admin	Remove ZoneDirector administration privileges from a user role

Defaults

None.

Example

```
ruckus(config-role)# no admin
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

admin

To add ZoneDirector administration privileges to a user role, use the following command:

```
admin [super | operator | monitoring]
```

Syntax Description

admin	Add ZoneDirector administration privileges to a user role
super	Sets to Super (Perform all configuration and management tasks)
operator	Sets to Operator (Change settings affecting single AP's only)
monitoring	Sets to Monitoring (Monitoring and viewing operation status only)

Defaults

None.

Example

```
ruckus(config-role)# admin super
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

show

To display the settings of a role, use the following command:

```
show
```

Syntax Description

show	Display the settings of a role

Defaults

None.

Example

```
ruckus(config-role)# show
Role:
  ID:
    :
      Name= role1
      Description=
      Group Attributes=
      Guest Pass Generation= Disallowed
      ZoneDirector Administration:
        Status= Disallowed
      Allow All WLANs:
        Mode= Allow Specify WLAN access

ruckus(config-role)#
```

Configure User Commands

Use the `user` commands to configure a user's name, password, and role.To run these commands, you must first enter the `config-user` context.

user

To create a user or modify an existing user and enter the `config-user` context, use the `following command:`

```
user <WORD>
```

Syntax Description

user	Create or modify a user entry
<WORD>	Name of the user

Defaults

None.

Example

```
rruckus(config)# user johndoe
The User entry 'johndoe' has been created.
ruckus(config-user)#
```

no user

To delete a user record, use the following command:

```
no user <WORD>
```

Syntax Description

user	Create or modify a user entry
<WORD>	Name of the user

Defaults

None.

Example

```
ruckus(config)# no user johndoe
The User 'johndoe' has been deleted.
ruckus(config)#
```

abort

To exit the `config-user` context without saving changes, use the `abort` command. Enter this command from within the context of the user that you are configuring.

```
abort
```

Syntax Description

abort	Exit the user settings without saving changes

Defaults

None.

Example

```
ruckus(config-user)# abort
No changes have been saved.
ruckus(config)#
```

end

To save changes, and then exit the `config-user` context, use the following command:

```
end
```

Syntax Description

end	Save changes, and then exit the context

Defaults

None.

Example

```
ruckus(config-user)# end
The User entry has saved successfully.
Your changes have been saved.
ruckus(config)#
```

exit

To save changes, and then exit the `config-user` context, use the following command:

```
exit
```

Syntax Description

exit	Save changes, and then exit the context

Defaults

None.

Example

```
ruckus(config-user)# exit
The User entry has saved successfully.
Your changes have been saved.
ruckus(config)#
```

quit

To exit the `config-user` context without saving changes, use the `quit` command. Enter this command from within the context of the user that you are configuring.

```
quit
```

Syntax Description

quit	Exit the user settings without saving changes

Defaults

None.

Example

```
ruckus(config-role)# quit
No changes have been saved.
ruckus(config)#
```

user-name

To set the name of a user, use the following command:

```
user-name <user_name>
```

Syntax Description

user-name	Set the name of a user
<user_name>	Set to this user name

Defaults

None.

Example

```
ruckus(config-user)# user-name joe1
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

full-name

To set the full name of a user, use the following command:

```
full-name <WORD>
```

Syntax Description

full-name	Set the full name of a user
<WORD>	Set to this full name

Defaults

None.

Example

```
ruckus(config-user)# full-name joejoe
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

password

To set the password of a user, use the following command:

```
password <WORD>
```

Syntax Description

password	Set the password of a user
<WORD>	Set to this password

Defaults

None.

Example

```
ruckus(config-user)# password 1234
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

role

To assign a role to a user, use the following command:

```
role <WORD>
```

Syntax Description

role	Assign a role to a user
<WORD>	Assign this role

Defaults None.

Example

```
ruckus(config-user)# role guest
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

show

To display the settings of a user, use the following command:

```
show
```

Syntax Description

show	Show user settings

Defaults None.

Example

```
ruckus(config-user)# show
User:
ID:
:
User Name= joe1
Full Name= joejoe
Password= 1234
Role= guest
```

Configure Guest Access Commands

Use the `guest-access` commands to configure the guest access settings. To run these commands, you must first enter the `config-guest-access` context.

guest-access

To configure Guest Access settings and enter the config-guest-access context, use the following command:

```
guest-access
```

Example

```
ruckus(config)# guest-access
ruckus(config-guest-access)#
```

abort

To exit the `config-guest-access` context without saving changes, use the `abort` command.

```
abort
```

Syntax Description

abort	Exit the guest access settings without saving changes

Defaults

None.

Example

```
ruckus(config-guest-access)# abort
No changes have been saved.
ruckus(config)#
```

end

To save changes, and then exit the `config-guest-access` context, use the following command:

```
end
```

Syntax Description

end	Save changes, and then exit the context

Defaults

None.

Example

```
ruckus(config-guest-access)# end
```

```
Your changes have been saved.
ruckus(config)#
```

exit

To save changes, and then exit the `config-guest-access` context, use the following command:

```
exit
```

Syntax Description

exit	Save changes, and then exit the context

Defaults

None.

Example

```
ruckus(config-guest-access)# exit
Your changes have been saved.
ruckus(config)#
```

quit

To exit the `config-guest-access` context without saving changes, use the `quit` command.

```
quit
```

Syntax Description

quit	Exit the guest access settings without saving changes

Defaults

None.

Example

```
ruckus(config-guest-access)# quit
No changes have been saved.
ruckus(config)#
```

no authentication

To disable guest access authentication, use the following command:

```
no authentication
```

Syntax Description

exit	Disable guest access authentication

Defaults

None.

Example

```
ruckus(config-guest-access)# no authentication
The command was executed successfully.
```

authentication guest-pass

To allow multiple users to share a single guest pass, use the following command:

```
authentication guest-pass [shared | no-shared]
```

Syntax Description

authentication guest-pass	Configure guest pass authentication
shared	Allow multiple users to share a single guest pass
no-shared	Allow only a single user to use a guest pass

Defaults

None.

Example

```
ruckus(config-guest-access)# authentication guest-pass shared
The command was executed successfully.
```

no term-of-use

To hide the Terms of Use text on the guest pass access page, use the following command:

```
no term-of-use
```

Syntax Description

no term-of-use	Hide Terms of Use

Defaults

None.

Example

```
ruckus(config-guest-access)# no term-of-use
The command was executed successfully.
```

term-of-use

To display and specify the Terms of Use text on the guest pass access page, use the following command:

```
term-of-use <term_of_use_text>
```

Syntax Description

term-of-use	Display Terms of Use
<term_of_use_text>	Use this text

Defaults None.

Example

```
ruckus(config-guest-access)# term-of-use test.guest
The command was executed successfully.
```

redirect

To set the URL to which to redirect a guest user after passing authentication, use the following command:

```
redirect [original | url <start_page_url>]
```

Syntax Description

redirect	Set the URL to which the guest user will be redirected
original	Redirect user to the original page that he intended to visit
url <start_page_url>	Redirect user to a different URL. Specify the URL in `<start_page_url>`.

Defaults original

Example

```
ruckus(config-guest-access)# redirect url
http://www.ruckuswireless.com
The command was executed successfully.
```

auth-server

To set the authentication server for guest user authentication, use the following command:

```
auth-server [local | name <auth_server_name>]
```

Syntax Description

auth-server	Set the authentication server for guest users
local	Use the controller as the authentication server
name <auth_server_name>	Use an external authentication server. Specify the authentication server name in `<auth_server_name>`.

Defaults local

Example

```
ruckus(config-guest-access)# auth-server local
The command was executed successfully.
```

guestpass-effective

To set the duration during which the guest pass will be effective, use the following command:

```
guestpass-effective [now | first-use-expired <NUMBER>]
```

Syntax Description

guestpass-effective	Set the guest pass effectivity period
now	Set the guest pass effective as soon as it is generated
first-use-expired <NUMBER>	Set the guest pass to be effective upon first use and to expire after a specified number of days.

Defaults

now

Example

```
ruckus(config-guest-access)# guestpass-effective first-use-expired 4
The command was executed successfully.
```

welcome-text

To configure the text to display on the guest access user login page, use the following command:

```
welcome-text <WORD>
```

Syntax Description

welcome-text	Configure the welcome message
<WORD>	Use this as the welcome message

Defaults

Welcome to the Guest Access login page.

Example

```
ruckus(config-guest-access)# welcome-text "Welcome to the Guest Access Login Page"
The command was executed successfully.
ruckus(config-guest-access)#
```

show

To display the guest pass settings, use the following command:

```
show
```

Syntax Description

show	Display the guest pass settings

Defaults

None.

Example

```
ruckus(config-guest-access)# show
Guest Access:
  Authentication:
    Mode= Use guest pass authentication
    Multiple users to share a single guest pass= Disallowed
  Terms of Use:
    Status= Disabled
  Redirection:
    Mode= To the URL that the user intends to visit
  Authentication Server= Local Database
  Validity Period:
    Mode= Effective from the creation time
  Title= Welcome to the Guest Access Login Page
  Restricted Subnet Access:
      Name= Guest
      Description=
      Default Action if no rule is matched= Deny all by default
      Rules:
        1:
          Description=
          Type= Deny
          Destination Address= local
          Destination Port= Any
          Protocol= Any
        2:
          Description=
          Type= Deny
          Destination Address= 10.0.0.0/8
          Destination Port= Any
          Protocol= Any
        3:
          Description=
          Type= Deny
          Destination Address= 172.16.0.0/12
          Destination Port= Any
          Protocol= Any
        4:
          Description=
          Type= Deny
          Destination Address= 192.168.0.0/16
```

```
            Destination Port= Any
            Protocol= Any

    Restricted IPv6 Access:
        Name= Guest
        Description=
        Default Action if no rule is matched= Deny all by default
        Rules:
          1:
            Description=
            Type= Deny
            Destination Address= local
            Destination Port= Any
            Protocol= Any
            ICMPv6 Type= Any

ruckus(config-guest-access)#
```

Guest Access Restriction Commands

Use the `guest-restrict-access` commands to configure network segments to which guest access will be blocked. To run these commands, you must first enter the `config-guest-restrict-access` context.

no restrict-access-order

To delete a restrict access order, use the following command:

```
no restrict-access-order <NUMBER>
```

Syntax Description

no restrict-access-order	Delete a restrict access order
<NUMBER>	Delete this order ID

Defaults

None.

Example

```
ruckus(config-guest-access)# no restrict-access-order 4
The Restricted Subnet Access entry has been removed from the Guest
Access.
```

restrict-access-order

To create a new restrict access order or modify an existing restrict access order, use the following command:

```
restrict-access-order <NUMBER>
```

This command enters the config-guest-restrict-access context. The following commands are available from within this context:

Syntax Description

help	Shows available commands
history	Shows a list of previously run commands.
abort	Exits the config-guest-restrict-access context without saving changes.
end	Saves changes, and then exits the config-guest-restrict-access context.
exit	Saves changes, and then exits the config-guest-restrict-access context.
quit	Exits the config-guest-restrict-access context without saving changes.
order <NUMBER>	Sets the guest access rule order.
description <WORD>	Sets the guest access rule description.
type [allow | deny]	Sets the guest access rule type to allow or deny.
destination [address <ADDR> | port <NUMBER/WORD>	Sets the destination address/port of a guest access rule.
protocol <NUMBER/WORD>	Sets the protocol of a guest access rule.
show	Displays restricted subnet access settings.

abort

To exit the `config-guest-restrict-access` context without saving changes, use the `abort` command.

```
abort
```

Syntax Description

abort	Exit the guest access restriction settings without saving changes

Defaults

None.

Example

```
ruckus(config-guest-restrict-access)# abort
No changes have been saved.
ruckus(config-guest-access)#
```

end

To save changes, and then exit the `config-guest-restrict-access` context, use the following command:

```
end
```

Syntax Description

end	Save changes, and then exit the context

Defaults

None.

Example

```
ruckus(config-guest-restrict-access)# end
The Restricted Subnet Access entry has been added to the Guest
Access.
Your changes have been saved.
ruckus(config-guest-access)#
```

exit

To save changes, and then exit the `config-guest-restrict-access` context, use the following command:

```
exit
```

Syntax Description

exit	Save changes, and then exit the context

Defaults

None.

Example

```
ruckus(config-guest-restrict-access)# exit
The Restricted Subnet Access entry has been added to the Guest
Access.
Your changes have been saved.
ruckus(config-guest-access)#
```

quit

To exit the `config-guest-restrict-access` context without saving changes, use the `quit` command.

```
quit
```

Syntax Description

quit	Exit the guest access restriction settings without saving changes

Defaults

None.

Example

```
ruckus(config-guest-restrict-access)# quit
No changes have been saved.
ruckus(config-guest-access)#
```

show

To display guest access restriction settings, use the following command:

```
show
```

Syntax Description

show	Display guest access restriction settings

Defaults

None.

order

To configure the guest access rule order, use the following command:

```
order <NUMBER>
```

Syntax Description

order	Set the order of a guest access rule
<NUMBER>	Assign the rule this order

Defaults

None.

Example

```
ruckus(config-guest-restrict-access)# order 3
The command was executed successfully.
```

description

To set the description of a guest access rule, use the following command:

```
description <WORD>
```

Syntax Description

description	Set the description of a guest access rule
<WORD>	Set this as description

Defaults None.

Example

```
ruckus(config-guest-restrict-access)# description guestd3
The command was executed successfully.
```

type allow

To set the guest access rule type to 'allow', use the following command:

```
type allow
```

Syntax Description

type	Set the guest access rule type
allow	Set the rule type to 'allow'

Defaults None.

Example

```
ruckus(config-guest-restrict-access)# type allow
The command was executed successfully.
```

type deny

To set the guest access rule type to 'deny', use the following command:

```
type deny
```

Syntax Description

type	Set the guest access rule type
deny	Set the rule type to 'deny'

Defaults None.

Example

```
ruckus(config-guest-restrict-access)# type deny
The command was executed successfully.
```

destination address

To set the destination address of the rule, use the following command:

```
destination address <IP-ADDR/WORD>
```

Syntax Description

destination address	Set the destination address of the rule
IP-ADDR/WORD	Set the destination to this IP address

Defaults None.

Example
```
ruckus(config-guest-restrict-access)# destination address
192.168.0.20/24
The command was executed successfully.
```

destination port

To set the destination port of the rule, use the following command:

```
destination port <NUMBER/WORD>
```

Syntax Description

destination port	Set the destination port of the rule
<NUMBER/WORD>	Set the destination to this port number

Defaults None.

Example
```
ruckus(config-guest-restrict-access)# destination port 562
The command was executed successfully.
```

protocol

To set the protocol for the rule, use the following command:

```
protocol <NUMBER/WORD>
```

Syntax Description

protocol	Set the protocol for the rule
<NUMBER/WORD>	Set to this protocol

Defaults None.

Example
```
ruckus(config-guest-restrict-access)# protocol 69
The command was executed successfully.
```

IPv6 Guest Restrict Access Commands

Use the IPv6 guest restrict access commands to configure IPv6 network segments to which guest access will be blocked. To run these commands, you must first enter the `config-ipv6-guest-restrict-access` context.

no restrict-access-order-ipv6

To delete a restrict access order, use the following command:

```
no restrict-access-order-ipv6 <NUMBER>
```

Syntax Description

no restrict-access-order-ipv6	Delete a restrict access order
<NUMBER>	Delete this order ID

Defaults

None.

Example

```
ruckus(config-guest-access)# no restrict-access-order-ipv6 2
The IPv6 Restricted Subnet Access entry has been removed from the
Guest Access.
ruckus(config-guest-access)#
```

restrict-access-order-ipv6

To create a new restrict access order or modify an existing restrict access order, use the following command:

```
restrict-access-order-ipv6 <NUMBER>
```

This command enters the config-ipv6-guest-restrict-access context. The following commands are available from within this context:

Syntax Description

help	Shows available commands
history	Shows a list of previously run commands.
abort	Exits the config-guest-restrict-access context without saving changes.
end	Saves changes, and then exits the config-guest-restrict-access context.
exit	Saves changes, and then exits the config-guest-restrict-access context.
quit	Exits the config-guest-restrict-access context without saving changes.
order <NUMBER>	Sets the guest access rule order.
description <WORD>	Sets the guest access rule description.
type [allow | deny]	Sets the guest access rule type to allow or deny.

destination [address <IPv6-ADDR> | port <NUMBER/WORD>	Sets the destination address/port of a guest access rule.
protocol <NUMBER/WORD>	Sets the protocol of a guest access rule.
icmpv6-type	Sets the ICMPv6 type of a Guest Access rule.
show	Displays restricted subnet access settings.

Example

```
ruckus(config-guest-access)# restrict-access-order-ipv6 2
ruckus(config-ipv6-guest-restrict-access)# type allow
The command was executed successfully.
ruckus(config-ipv6-guest-restrict-access)# show
          Description=
          Type= Allow
          Destination Address= Any
          Destination Port= Any
          Protocol= Any
          ICMPv6 Type= Any
ruckus(config-ipv6-guest-restrict-access)# end
The IPv6 Restricted Subnet Access entry has been added to the Guest Access.
Your changes have been saved.
ruckus(config-guest-access)#
```

abort

To exit the `config-ipv6-guest-restrict-access` context without saving changes, use the `abort` command.

```
abort
```

Syntax Description

abort	Exit the guest access restriction settings without saving changes

Defaults

None.

Example

```
ruckus(config-ipv6-guest-restrict-access)# abort
No changes have been saved.
ruckus(config-guest-access)#
```

end

To save changes, and then exit the `config-ipv6-guest-restrict-access` context, use the following command:

```
end
```

Syntax Description

end	Save changes, and then exit the context

Defaults

None.

Example

```
ruckus(config-ipv6-guest-restrict-access)# end
The Restricted Subnet Access entry has been added to the Guest Access.
Your changes have been saved.
ruckus(config-guest-access)#
```

exit

To save changes, and then exit the `config-ipv6-guest-restrict-access` context, use the following command:

```
exit
```

Syntax Description

exit	Save changes, and then exit the context

Defaults

None.

Example

```
ruckus(config-ipv6-guest-restrict-access)# exit
The Restricted Subnet Access entry has been added to the Guest Access.
Your changes have been saved.
ruckus(config-guest-access)#
```

quit

To exit the `config-ipv6-guest-restrict-access` context without saving changes, use the `quit` command.

```
quit
```

Syntax Description

quit	Exit the guest access restriction settings without saving changes

Defaults None.

Example

```
ruckus(config-ipv6-guest-restrict-access)# quit
No changes have been saved.
ruckus(config-guest-access)#
```

show

To display guest access restriction settings, use the following command:

```
show
```

Syntax Description

show	Display guest access restriction settings

Example

```
ruckus(config-ipv6-guest-restrict-access)# show
          Description=
          Type= Allow
          Destination Address= Any
          Destination Port= Any
          Protocol= Any
          ICMPv6 Type= Any
ruckus(config-ipv6-guest-restrict-access)#
```

order

To configure the guest access rule order, use the following command:

```
order <NUMBER>
```

Syntax Description

order	Set the order of a guest access rule
<NUMBER>	Assign the rule this order

Defaults None.

Example

```
ruckus(config-ipv6-guest-restrict-access)# order 3
The command was executed successfully.
```

description

To set the description of a guest access rule, use the following command:

```
description <WORD>
```

Syntax Description

description	Set the description of a guest access rule
<WORD>	Set this as description

Defaults None.

Example

```
ruckus(config-ipv6-guest-restrict-access)# description guestd3
The command was executed successfully.
```

type allow

To set the guest access rule type to 'allow', use the following command:

```
type allow
```

Syntax Description

type	Set the guest access rule type
allow	Set the rule type to 'allow'

Defaults None.

Example

```
ruckus(config-ipv6-guest-restrict-access)# type allow
The command was executed successfully.
```

type deny

To set the guest access rule type to 'deny', use the following command:

```
type deny
```

Syntax Description

type	Set the guest access rule type
deny	Set the rule type to 'deny'

Defaults None.

Example

```
ruckus(config-ipv6-guest-restrict-access)# type deny
The command was executed successfully.
```

destination address

To set the destination address of the rule, use the following command:

```
destination address <IP-ADDR/WORD>
```

Syntax Description

destination address	Set the destination address of the rule
IP-ADDR/WORD	Set the destination to this IP address

Defaults None.

Example

```
ruckus(config-ipv6-guest-restrict-access)# destination address
fe80::/64
The command was executed successfully.
ruckus(config-ipv6-guest-restrict-access)#
```

destination port

To set the destination port of the rule, use the following command:

```
destination port <NUMBER/WORD>
```

Syntax Description

destination port	Set the destination port of the rule
<NUMBER/WORD>	Set the destination to this port number

Defaults None.

Example

```
ruckus(config-ipv6-guest-restrict-access)# destination port 562
The command was executed successfully.
```

protocol

To set the protocol for the rule, use the following command:

```
protocol <NUMBER/WORD>
```

Syntax Description

protocol	Set the protocol for the rule
<NUMBER/WORD>	Set to this protocol

Defaults None.

Example

```
ruckus(config-ipv6-guest-restrict-access)# protocol 69
The command was executed successfully.
```

icmpv6-type

To set the ICMPv6 type of a Guest Access rule, use the following command:

```
icmpv6-type [any | number <NUMBER>]
```

Defaults

Any.

Example

```
ruckus(config-ipv6-guest-restrict-access)# icmpv6-type any
The command was executed successfully.
ruckus(config-ipv6-guest-restrict-access)#
```

Configure Hotspot Commands

Use the `hotspot` commands to configure the controller's hotspot settings. To run these commands, you must first enter the `config-hotspot` context.

hotspot

To create a new hotspot or edit an existing entry and enter the config-hotspot context, use the following command:

```
hotspot <WORD>
```

Syntax Description

hotspot	Create or edit a hotspot service
<WORD>	Name of hotspot service

Defaults

None.

Example

```
ruckus(config)# hotspot hotspot1
The Hotspot entry 'hotspot1' has been loaded. To save the Hotspot
entry, type end or exit.
ruckus(config-hotspot)#
```

no hotspot

To delete a hotspot record from the list, use the following command:

```
no hotspot <WORD>
```

Syntax Description

hotspot	Create or edit a hotspot service
<WORD>	Name of hotspot service

Defaults

None.

Example

```
ruckus(config)# hotspot hotspot1
The Hotspot entry 'hotspot1' has been loaded. To save the Hotspot
entry, type end or exit.
ruckus(config-hotspot)#
```

abort

To exit the `config-hotspot` context without saving changes, use the `abort` command.

```
abort
```

Syntax Description

abort	Exit the hotspot settings without saving changes

Defaults

None.

Example

```
ruckus(config-hotspot)# abort
No changes have been saved.
ruckus(config)#
```

end

To save changes, and then exit the `config-hotspot` context, use the following command:

```
end
```

Syntax Description

end	Save changes, and then exit the context

Defaults

None.

Example

```
ruckus(config-hotspot)# end
The login page url can't be empty.
ruckus(config-hotspot)# end
The Hotspot entry has saved successfully.
Your changes have been saved.
ruckus(config)#
```

exit

To save changes, and then exit the `config-hotspot` context, use the following command:

```
exit
```

Syntax Description

exit	Save changes, and then exit the context

Defaults

None.

Example

```
ruckus(config-hotspot)# exit
The login page url can't be empty
ruckus(config-hotspot)# exit
The Hotspot entry has saved successfully.
Your changes have been saved.
```

quit

To exit the `config-hotspot` context without saving changes, use the `quit` command.

```
quit
```

Syntax Description

quit	Exit the hotspot settings without saving changes

Defaults

None.

Example

```
ruckus(config-hotspot)# quit
No changes have been saved.
ruckus(config)#
```

show

To display the current hotspot settings, use the following command:

```
show
```

Syntax Description

show	Display the current hotspot settings

Defaults

None.

Example

```
ruckus(config-hotspot)# show
Hotspot:
ID:
1:
```

```
Name= h1
Login Page Url= http://172.18.110.122
Start Page= redirect to the URL that the user intends to visit.
Session Timeout= Disabled
Idle Timeout= Enabled
Timeout= 60 Minutes
Authentication Server= Local Database
Accounting Server= Disabled
Location ID=
Location Name=
Walled Garden 1=
Walled Garden 2=
Walled Garden 3=
Walled Garden 4=
Walled Garden 5=
Rules:
Order= 1
Description= h1_order1
Type= Deny
Destination Address= 192.168.20.20/24
Destination Port= 920
Protocol= 58
```

name

To set the hotspot name, use the following command

```
name <WORD>
```

Syntax Description

name	Set the hotspot name
<WORD>	Set to this name

Defaults

None.

Example

```
ruckus(config-hotspot)# name ruckus1
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

smartclient

Use the following command to enable WISPr smart client support

```
smartclient [secure https] [secure http] [wispr-only secure
https] [wispr-only secure-http] [info]
```

Syntax Description

`smartclient`	Enable WISPr smartclient support
secure https	Enables WISPr smart client support with HTTPS security.
secure http	Enables WISPr smart client support with no security.
wispr-only secure https	Enables only WISPr smart client support with HTTPS security.
wispr-only secure http	Enables only WISPr smart client support with no security.
info	Sets the instruction to guide user to login by Smart Client application.

Defaults

None.

Example

```
ruckus(config-hotspot)# smartclient secure https
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-hotspot)#
```

no smartclient

To disable WISPr Smart Client support, use the following command:

```
no smartclient
```

login-page

To set the URL of the hotspot login, use the following command:

```
login-page [original|<WORD>]
```

Syntax Description

login-page	Set the URL of the hotspot login
<WORD>	Set to this URL
original	Redirect to the URL that the user intends to visit

Defaults

None.

Example

```
ruckus(config-hotspot)# login-page http://ruckuswireless.com
```

```
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

start-page

To set the URL or page to which the user will be redirected after logging into the hotspot, use the following command:

```
start-page [original | url <WORD>]
```

Syntax Description

start-page	Set the URL or page to which the user will be redirected after logging into the hotspot
original	Redirect user to the original page he or she intended to visit
url <WORD>	Redirect use to another page. Set the URL of the page in <WORD>.

Defaults

original

Example

```
ruckus(config-hotspot)# start-page url
http://www.ruckuswireless.com
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

no session-timeout

To disable the session timeout for hotspot usage, use the following command:

```
no session-timeout
```

Syntax Description

no session-timeout	Disable the session timeout for hotspot usage

Defaults

None.

Example

```
ruckus(config-hotspot)# no session-timeout
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

session-timeout

To enable and set the session timeout for hotspot usage, use the following command:

```
session-timeout <minutes>
```

Syntax Description

session-timeout	Disable the session timeout for hotspot usage
<minutes>	Set the session timeout to this value (in minutes)

Defaults

1440 minutes

Example

```
ruckus(config-hotspot)# session-timeout 20
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

no grace-period

To disable the grace period (idle timeout) for hotspot users, use the following command:

```
no grace-period
```

Syntax Description

no grace-period	Disable the idle timeout for hotspot users

Defaults

None.

Example

```
ruckus(config-hotspot)# no grace-period
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

grace-period

To enable and set the grace period (idle timeout) for hotspot users, use the following command:

```
grace-period <minutes>
```

Syntax Description

grace-period	Set the idle timeout for hotspot users
<minutes>	Set the idle timeout to this value (in minutes)

Defaults

60 minutes

Example

```
ruckus(config-hotspot)# grace-period 20
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

auth-server local

To use ZoneDirector as the authentication server for hotspot users, use the following command:

```
auth-server local
```

Syntax Description

auth-server	Set an authentication server for hotspot users
local	Use ZoneDirector as the authentication server

Defaults

local

Example

```
ruckus(config-hotspot)# auth-server local
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

auth-server name

To use an external server for authenticating hotspot users, use the following command:

```
auth-server name <WORD>
```

Syntax Description

auth-server name	Set an external authentication server for hotspot users
<WORD>	Use this server as the authentication server

Defaults

None.

Example

```
ruckus(config-hotspot)# auth-server name radius1
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-hotspot)#
```

auth-server name mac-bypass

To enable MAC authentication bypass (no redirection) and use password as authentication password, use the following command:

```
auth-server name <WORD> mac-bypass password <WORD>
```

Syntax Description

auth-server name	Set an external authentication server for hotspot users

<WORD>	Authentication server name
mac-bypass	Enable MAC auth bypass
mac	Enables MAC authentication bypass (no redirection) and use device MAC address as authentication password.
password <WORD>	Enables MAC authentication bypass (no redirection) and use password as authentication password.
mac-in-dot1x	Use device MAC address as authentication password and enable to send username and password in 802.1X format of 00-10-A4-23-19-C0 (by default 0010a42319c0).
password-in-dot1x <WORD>	Use password as authentication password and enable to send username and password in 802.1X format of 00-10-A4-23-19-C0 (by default 0010a42319c0).

Defaults

None.

Example

```
ruckus(config-hotspot)# auth-server name radius1 mac-bypass mac
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-hotspot)#
```

acct-server

To enable the accounting server for hotspot usage, use the following command:

```
acct-server <WORD>
```

Syntax Description

acct-server	Enable the accounting server for hotspot usage
<WORD>	Name of the AAA server

Defaults

None.

Example

```
ruckus(config-hotspot)# acct-server "RADIUS Accounting"
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-hotspot)#
```

no acct-server

To disable the accounting server for hotspot usage, use the following command:

```
no acct-server
```

Syntax Description

no acct-server	Disable the accounting server for hotspot usage

Defaults

None.

Example

```
ruckus(config-hotspot)# no acct-server
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

acct-server interim-update

To enable and set the accounting server for hotspot usage, use the following command:

```
acct-server <WORD> interim-update <NUMBER>
```

Syntax Description

no acct-server	Enable and set the accounting server for hotspot usage
<WORD>	Set to this accounting server
interim-update	Set the interim update interval
<NUMBER>	Set to this interval (in minutes)

Defaults

5 minutes

Example

```
ruckus(config-hotspot)# acct-server asd interim-update 10
The AAA server 'asd' could not be found. Please check the spelling,
and then try again.
ruckus(config-hotspot)# acct-server acct1 interim-update 20
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

client-isolation

To enable wireless client isolation and set the level of isolation, use the following command:

```
client-isolation [local | full]
```

Syntax Description

client-isolation	Enable client isolation
local	Set client isolation to local. Wireless clients associated with the same AP will be unable to communicate with one another locally.
full	Set client isolation to full. Wireless clients will be unable to communicate with each other or access any of the restricted subnets.

Defaults

None

Example

```
ruckus(config-hotspot)# client-isolation local
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-hotspot)#
```

no client-isolation

To disable wireless client isolation, use the following command:

```
no client-isolation
```

Example

```
ruckus(config-hotspot)# no lient-isolation
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-hotspot)#
```

location-id

To set the location ID of the hotspot, use the following command:

```
location-id <location-id>
```

Syntax Description

location-id	Set the location ID of the hotspot
<location-id>	Set to this location ID

Defaults

None.

Example

```
ruckus(config-hotspot)# location-id us
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

location-name

To set the location name of the hotspot, use the following command:

```
location-name <location-name>
```

Syntax Description

`location-name`	Set the location name of the hotspot
`<location-name>`	Set to this location name

Defaults

None.

Example

```
ruckus(config-hotspot)# location-name shenzhen
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

walled-garden

To set a hotspot "walled garden" URL, use the following command:

```
walled-garden <INDEX> <WORD>
```

Syntax Description

`walled-garden`	Create a walled garden rule
`<INDEX>`	Enter walled garden URL index. (1~35)
`<WORD>`	Destination URL

Defaults

None.

Example

```
ruckus(config-hotspot)# walled-garden 1 www.ruckuswireless.com
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-hotspot)#
```

no walled-garden

To delete a walled garden URL, use the following command

```
no walled-garden <INDEX>
```

Syntax Description

`walled-garden`	Delete a walled garden rule
`<INDEX>`	Enter walled garden URL index. (1~35)

Defaults

None.

Example

```
ruckus(config-hotspot)# no walled-garden 1
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-hotspot)#
```

Configuring Hotspot Restricted Access Rules

The following commands are used to create and modify Hotspot restricted access rules. Use the restrict-access-order command from the config-hotspot context to enter the config-hotspot-restrict-access context.

restrict-access-order

To create a new restrict access order or modify an existing restrict access order, use the following command:

```
restrict-access-order <NUMBER>
```

Syntax Description

restrict-access-order	Add a restrict access order
<NUMBER>	Add this order ID
order <NUMBER>	Sets the hotspot rule order.
description <WORD>	Sets the hotspot rule description.
type allow	Sets the hotspot rule type to 'allow'.
type deny	Sets the hotspot rule type to 'deny'.
destination address <IP-ADDR/ WORD>	Sets the destination address of a hotspot rule.
destination port <NUMBER/ WORD>	Sets the destination port of a hotspot rule.
protocol <NUMBER/WORD>	Sets the protocol of a hotspot rule.
show	Displays the policy rule.

Defaults

None.

Example

```
ruckus(config-hotspot)# restrict-access-order 1
ruckus(config-hotspot-restrict-access)#
ruckus(config-hotspot-restrict-access)# show
          Description=
          Type= Deny
```

```
          Destination Address= Any
          Destination Port= Any
          Protocol= Any
ruckus(config-hotspot-restrict-access)#
```

no restrict-access-order

To delete a restrict access order, use the following command:

```
no restrict-access-order <NUMBER>
```

Syntax Description

`no restrict-access-order`	Delete a restrict access order
`<NUMBER>`	Delete this order ID

Defaults

None.

Example

```
ruckus(config-hotspot)# no restrict-access-order 1
The rule '1' has been removed from the Hotspot.
```

restrict-access-order-ipv6

To create a new IPv6 restrict access order or modify an existing restrict access order, use the following command:

```
restrict-access-order-ipv6 <NUMBER>
```

Syntax Description

`restrict-access-order-ipv6`	Add a restrict access order
`<NUMBER>`	Add this order ID
order <NUMBER>	Sets the hotspot rule order.
description <WORD>	Sets the hotspot rule description.
type allow	Sets the hotspot rule type to 'allow'.
type deny	Sets the hotspot rule type to 'deny'.
destination address <IP-ADDR/WORD>	Sets the destination address of a hotspot rule.
destination port <NUMBER/WORD>	Sets the destination port of a hotspot rule.
protocol <NUMBER/WORD>	Sets the protocol of a hotspot rule.
`icmpv6 type [any|number <NUMBER>]`	Sets the icmpv6 type of a hotspot rule.

show	Displays the policy rule.

Defaults

None.

Example

```
ruckus(config-hotspot)# restrict-access-order-ipv6 1
ruckus(config-hotspot-restrict-access)#
ruckus(config-hotspot-restrict-access-ipv6)# show
          Description=
          Type= Deny
          Destination Address= Any
          Destination Port= Any
          Protocol= Any
          ICMPv6 Type= Any
ruckus(config-hotspot-restrict-access-ipv6)#
```

no restrict-access-order-ipv6

To delete a restrict access order, use the following command:

```
no restrict-access-order-ipv6 <order_id>
```

Syntax Description

`no restrict-access-order`	Delete a restrict access order
`<order_id>`	Delete this order ID

Defaults

None.

Example

```
ruckus(config-hotspot)# no restrict-access-order-ipv6 1
The rule '1' has been removed from the Hotspot.
```

icmpv6-type

To set the ICMPv6 type, use the following command:

```
icmpv6-type [any | number <NUMBER>]
```

Defaults

Any.

Example

```
ruckus(config-hotspot-restrict-access-ipv6)# icmpv6-type any
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-hotspot-restrict-access-ipv6)#
```

Hotspot Access Restriction Commands

Use the `hotspot-restrict-access` commands to configure network segments to which hotspot access will be blocked. To run these commands, you must first enter the `config-hotspot-restrict-access` context.

The same commands are available for IPv6 networks from the `config-hotspot-restrict-access-ipv6` context.

end

To save changes, and then exit the `config-hotspot-restrict-access` context, use the following command:

```
end
```

Syntax Description

end	Save changes, and then exit the context

Defaults

None.

Example

```
ruckus(config-hotspot-restrict-access)# end
ruckus(config-hotspot)#
```

exit

To save changes, and then exit the `config-hotspot-restrict-access` context, use the following command:

```
exit
```

Syntax Description

exit	Save changes, and then exit the context

Defaults

None.

Example

```
ruckus(config-hotspot-restrict-access)# exit
ruckus(config-hotspot)#
```

show

To display hotspot access restriction settings, use the following command:

```
show
```

Syntax Description

show	Display the hotspot access restriction settings

Defaults None.

order

To configure the hotspot access rule order, use the following command:

```
order <NUMBER>
```

Syntax Description

order	Set the order of a hotspot access rule
<NUMBER>	Assign the rule this order

Defaults None.

Example

```
ruckus(config-hotspot-restrict-access)# order 1
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

description

To set the description of a hotspot access rule, use the following command:

```
description <WORD>
```

Syntax Description

description	Set the description of a hotspot access rule
<WORD>	Set this as description

Defaults None.

Example

```
ruckus(config-hotspot-restrict-access)# description h1_order1
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

type allow

To set the hotspot access rule type to 'allow', use the following command:

```
type allow
```

Syntax Description

type	Set the hotspot access rule type

allow	Set the rule type to 'allow'

Defaults

None.

Example

```
ruckus(config-hotspot-restrict-access)# type allow
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

type deny

To set the hotspot access rule type to 'deny', use the following command:

```
type deny
```

Syntax Description

type	Set the hotspot access rule type
deny	Set the rule type to 'deny'

Defaults

None.

Example

```
ruckus(config-hotspot-restrict-access)# type deny
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

destination address

To set the destination address of the rule, use the following command:

```
destination address <IP-ADDR/WORD>
```

Syntax Description

destination address	Set the destination address of the rule
IP-ADDR/WORD	Set the destination to this IP address

Defaults

None.

Example

```
ruckus(config-hotspot-restrict-access)# destination address
192.168.20.20/24
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

destination port

To set the destination port of the rule, use the following command:

```
destination port <NUMBER/WORD>
```

Syntax Description

destination port	Set the destination port of the rule
<NUMBER/WORD>	Set the destination to this port number

Defaults

None.

Example

```
ruckus(config-hotspot-restrict-access)# destination port 920
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

protocol

To set the protocol for the rule, use the following command:

```
protocol <NUMBER/WORD>
```

Syntax Description

protocol	Set the protocol for the rule
<NUMBER/WORD>	Set to this protocol

Defaults

None.

Example

```
ruckus(config-hotspot-restrict-access)# protocol 58
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

intrusion-prevention

To enable temporary blocking of Hotspot clients with repeated authentication attempts, use the following command:

```
intrusion-prevention
```

Defaults

Disabled.

Example

```
ruckus(config-hotspot)# intrusion-prevention
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-hotspot)#
```

no intrusion-prevention

To disable temporary blocking of Hotspot clients with repeated authentication failure, use the following command:

```
no intrusion-prevention
```

Example

```
ruckus(config-hotspot)# no intrusion-prevention
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-hotspot)#
```

Configure Hotspot 2.0 Commands

Use the `hs20op` and `hs20sp` commands to configure the controller's Hotspot 2.0 operator and service provider settings. To run these commands, you must first enter the `config-hs20op` or `config-hs20sp` context.

To deploy a Hotspot 2.0 service, you must configure the following:

- A Hotspot 2.0 Operator entry
- A Hotspot 2.0 Service Provider entry
- A WLAN with Hotspot 2.0 service enabled

hs20op

Use the following command to configure a Hotspot 2.0 Operator entry:

```
hs20op <WORD>
```

Syntax Description

hs20op	Create or configure a Hotspot 2.0 Operator entry
<WORD>	The name of the Hotspot 2.0 Operator entry.

Example

```
ruckus(config)# hs20op operator1
The Hotspot (2.0) operator entry 'operator1' has been created.
ruckus(config-hs20op)# end
The Hotspot (2.0) operator entry has saved successfully.
Your changes have been saved.
ruckus(config)#
```

no hs20op

Use the following command to delete a Hotspot 2.0 Operator entry:

```
no hs20op <WORD>
```

Example

```
ruckus(config)# no hs20op operator1
```

```
The Hotspot (2.0) oeprator 'operator1' has been deleted.
ruckus(config)#
```

Configure Hotspot 2.0 Operator Settings

The following commands can be used to configure Hotspot 2.0 Operator entry settings. To execute these commands, you must first create or edit a Hotspot 2.0 Operator entry using the `hs20op` command and entering the `config-hs20op` context.

Syntax Description

help	Shows available commands.
history	Shows a list of previously run commands.
abort	Exits the config-hs20op context without saving changes.
end	Saves changes, and then exits the config-hs20op context.
exit	Saves changes, and then exits the config-hs20op context.
quit	Exits the config-hs20op context without saving changes.
no internet-option	Disables with connectivity to internet.
no hessid	Sets the HESSID to empty.
no service-provider <WORD>	Deletes a service provider from the Hotspot (2.0) operator.
no venue-group-type	Sets both venue group and venue type to unspecified.
no friendly-name <LANGUAGE>	Disable the friendly name for the specified language.
no asra	Disables additional step required for access.
no asra terms	Disables ASRA Type: Acceptance of terms and conditions.
no asra enrollment	Disables ASRA Type: On-line enrollment supported.
no asra http-https	Disables ASRA Type: http/https redirection.
no asra dns	Disables ASRA Type: DNS redirection.
no asra http-https-url	Sets the redirect URL of http/https redirection to empty.
no wan-metrics sym	Disables Symmetric Link.
no wan-metrics at-cap	Disables WAN at Capability.
no custm-conn-cap <NUMBER>	Deletes a Connection Capability entry.
no adv-gas dos-detect	Disables the GAS DOS detection.
no hs-caps operating-class-indication	Disables the operating class indication.
name <WORD>	Sets the hotspot(2.0) operator entry name.

description <WORD>	Sets the hotspot(2.0) operator entry description.
internet-option	Enables with connectivity to internet.
hessid <MAC>	Sets the HESSID.
hessid-use-bssid	Sets the HESSID to use BSSID.
service-provider <WORD>	Adds a service provider to the Hotspot (2.0) operator.
venue-group-type unspecified	Sets the venue group to unspecified
venue-group-type assembly	Sets the venue group to assembly
venue-group-type assembly unspecified	Sets the venue type to unspecified
venue-group-type assembly arena	Sets the venue type to arena
venue-group-type assembly stadium	Sets the venue type to stadium
venue-group-type assembly passenger-terminal	Sets the venue type to passenger terminal
venue-group-type assembly amphitheater	Sets the venue type to amphitheater
venue-group-type assembly amusement-park	Sets the venue type to amusement park
venue-group-type assembly place-worship	Sets the venue type to place of worship
venue-group-type assembly convention-center	Sets the venue type to convention center
venue-group-type assembly library	Sets the venue type to library
venue-group-type assembly museum	Sets the venue type to museum
venue-group-type assembly restaurant	Sets the venue type to restaurant
venue-group-type assembly theater	Sets the venue type to theater
venue-group-type assembly bar	Sets the venue type to bar

venue-group-type assembly coffee-shop	Sets the venue type to coffee shop
venue-group-type assembly zoo-or-aquarium	Sets the venue type to zoo or aquarium
venue-group-type assembly emergency-coordination-center	Sets the venue type to emergency coordination center
venue-group-type business	Sets the venue group to business
venue-group-type business unspecified	Sets the venue type to unspecified
venue-group-type business doctor-or-dentist-office	Sets the venue type to doctor or dentist office
venue-group-type business bank	Sets the venue type to bank
venue-group-type business fire-station	Sets the venue type to fire station
venue-group-type business police-station	Sets the venue type to police station
venue-group-type business post-office	Sets the venue type to post office
venue-group-type business professional-office	Sets the venue type to professional office
venue-group-type business research-and-development-facility	Sets the venue type to research and development facility
venue-group-type business attorney-office	Sets the venue type to attorney office
venue-group-type educational	Sets the venue group to educational
venue-group-type educational unspecified	Sets the venue type to unspecified
venue-group-type educational school-primary	Sets the venue type to school primary

venue-group-type educational school-secondary	Sets the venue type to school secondary
venue-group-type educational university-or-college	Sets the venue type to university or college
venue-group-type factory-industrial	Sets the venue group to factory industrial
venue-group-type factory-industrial unspecified	Sets the venue type to unspecified
venue-group-type factory-industrial factory	Sets the venue type to factory
venue-group-type institutional	Sets the venue group to institutional
venue-group-type institutional unspecified	Sets the venue type to unspecified
venue-group-type institutional hospital	Sets the venue type to hospital
venue-group-type institutional long-term-care-facility	Sets the venue type to long term care facility
venue-group-type institutional alcohol-and-drug-reHabilitation-center	Sets the venue type to alcohol and drug reHabilitation center
venue-group-type institutional group-home	Sets the venue type to group home
venue-group-type institutional prison-or-jail	Sets the venue type to prison or jail
venue-group-type mercantile	Sets the venue group to mercantile
venue-group-type mercantile unspecified	Sets the venue type to unspecified
venue-group-type mercantile retail-store	Sets the venue type to retail store
venue-group-type mercantile grocery-market	Sets the venue type to grocery market

venue-group-type mercantile automotive-service-station	Sets the venue type to automotive service station
venue-group-type mercantile shopping-mall	Sets the venue type to shopping mall
venue-group-type mercantile gas-station	Sets the venue type to gas station
venue-group-type residential	Sets the venue group to residential
venue-group-type residential unspecified	Sets the venue type to unspecified
venue-group-type residential private-residence	Sets the venue type to private residence
venue-group-type residential hotel-or-motel	Sets the venue type to hotel or motel
venue-group-type residential dormitory	Sets the venue type to dormitory
venue-group-type residential boarding-house	Sets the venue type to boarding house
venue-group-type storage	Sets the venue group to storage
venue-group-type storage unspecified	Sets the venue type to unspecified
venue-group-type utility-miscellaneous	Sets the venue group to utility miscellaneous
venue-group-type utility-miscellaneous unspecified	Sets the venue type to unspecified
venue-group-type vehicular	Sets the venue group to vehicular
venue-group-type vehicular unspecified	Sets the venue type to unspecified
venue-group-type vehicular automobile-or-truck	Sets the venue type to automobile or truck

venue-group-type vehicular airplane	Sets the venue type to airplane
venue-group-type vehicular bus	Sets the venue type to bus
venue-group-type vehicular ferry	Sets the venue type to ferry
venue-group-type vehicular ship-or-boat	Sets the venue type to ship or boat
venue-group-type vehicular train	Sets the venue type to train
venue-group-type vehicular motor-bike	Sets the venue type to motor bike
venue-group-type outdoor	Sets the venue group to outdoor
venue-group-type outdoor unspecified	Sets the venue type to unspecified
venue-group-type outdoor muni-mesh-network	Sets the venue type to muni mesh network
venue-group-type outdoor city-park	Sets the venue type to city park
venue-group-type outdoor rest-area	Sets the venue type to rest area
venue-group-type outdoor traffic-control	Sets the venue type to traffic control
venue-group-type outdoor bus-stop	Sets the venue type to bus stop
venue-group-type outdoor kiosk	Sets the venue type to kiosk
friendly-name <LANGUAGE> <WORD>	Sets the friendly name for the specified language.
asra	Enables additional step required for access.
asra terms	Enables ASRA Type: Acceptance of terms and conditions.
asra enrollment	Enables ASRA Type: On-line enrollment supported.
asra http-https	Enables ASRA Type: http/https redirection.
asra http-https url <WORD>	Sets the redirect URL of http/https redirection.
asra dns	Enables ASRA Type: DNS redirection.

accs-net-type private	Sets the access network type to Private network.
accs-net-type private-with-guest	Sets the access network type to Private network with guest access.
accs-net-type chargeable-public	Sets the access network type to Chargeable public network.
accs-net-type free-public	Sets the access network type to Free public network.
accs-net-type personal-device	Sets the access network type to Personal device network.
accs-net-type test-or-experimental	Sets the access network type to Test or experimental.
accs-net-type wildcard	Sets the access network type to Wildcard.
ip-addr-type ipv4 not-avail	Sets the IPv4 Address Type to not available.
ip-addr-type ipv4 public	Sets the IPv4 Address Type to public address.
ip-addr-type ipv4 port-restricted	Sets the IPv4 Address Type to port-restricted address.
ip-addr-type ipv4 single-nated	Sets the IPv4 Address Type to single NATed private address.
ip-addr-type ipv4 double-nated	Sets the IPv4 Address Type to double NATed private address.
ip-addr-type ipv4 port-single	Sets the IPv4 Address Type to port-restricted address and single NATed private address.
ip-addr-type ipv4 port-double	Sets the IPv4 Address Type to port-restricted address and double NATed private address.
ip-addr-type ipv4 unknown	Sets the IPv4 Address Type to unknown.
ip-addr-type ipv6 not-avail	Sets the IPv6 Address Type to not available.
ip-addr-type ipv6 avail	Sets the IPv6 Address Type to available.
ip-addr-type ipv6 unknown	Sets the IPv6 Address Type to unknown.
wan-metrics sym	Enables Symmetric Link.
wan-metrics at-cap	Enables WAN at Capability.
wan-metrics link-stat up	Sets Link Status to Link UP.
wan-metrics link-stat down	Sets Link Status to Link Down.
wan-metrics link-stat test	Sets Link Status to Link in Test State.

wan-metrics downlink-load <NUMBER>	Sets WAN downlink load.
wan-metrics downlink-speed <NUMBER>	Sets WAN downlink speed.
wan-metrics uplink-load <NUMBER>	Sets WAN uplink load.
wan-metrics uplink-speed <NUMBER>	Sets WAN uplink speed.
wan-metrics lmd <NUMBER>	Sets Load Measurement Duration.
conn-cap icmp closed	Sets the ICMP Connection Capability Status to closed
conn-cap icmp open	Sets the ICMP Connection Capability Status to open
conn-cap icmp unknown	Sets the ICMP Connection Capability Status to unknown
conn-cap ftp closed	Sets the FTP Connection Capability Status to closed
conn-cap ftp open	Sets the FTP Connection Capability Status to open
conn-cap ftp unknown	Sets the FTP Connection Capability Status to unknown
conn-cap ssh closed	Sets the SSH Connection Capability Status to clsoed
conn-cap ssh open	Sets the SSH Connection Capability Status to open
conn-cap ssh unknown	Sets the SSH Connection Capability Status to unknown
conn-cap http closed	Sets the HTTP Connection Capability Status to clsoed
conn-cap http open	Sets the HTTP Connection Capability Status to open
conn-cap http unknown	Sets the HTTP Connection Capability Status to unknown
conn-cap tls-vpn closed	Sets the TLS VPN Connection Capability Status to clsoed
conn-cap tls-vpn open	Sets the TLS VPN Connection Capability Status to open
conn-cap tls-vpn unknown	Sets the TLS VPN Connection Capability Status to unknown
conn-cap pptp-vpn closed	Sets the PPTP VPN Connection Capability Status to clsoed
conn-cap pptp-vpn open	Sets the PPTP VPN Connection Capability Status to open
conn-cap pptp-vpn unknown	Sets the PPTP VPN Connection Capability Status to unknown
conn-cap voip-tcp closed	Sets the VoIP(TCP) Connection Capability Status to closed
conn-cap voip-tcp open	Sets the VoIP(TCP) Connection Capability Status to open
conn-cap voip-tcp unknown	Sets the VoIP(TCP) Connection Capability Status to unknown
conn-cap ikev2 closed	Sets the IKEv2 Connection Capability Status to clsoed

conn-cap ikev2 open	Sets the IKEv2 Connection Capability Status to open
conn-cap ikev2 unknown	Sets the IKEv2 Connection Capability Status to unknown
conn-cap voip-udp closed	Sets the VoIP(UDP) Connection Capability Status to closed
conn-cap voip-udp open	Sets the VoIP(UDP) Connection Capability Status to open
conn-cap voip-udp unknown	Sets the VoIP(UDP) Connection Capability Status to unknown
conn-cap ipsec-vpn closed	Sets the IPSec VPN Connection Capability Status to clsoed
conn-cap ipsec-vpn open	Sets the IPSec VPN Connection Capability Status to open
conn-cap ipsec-vpn unknown	Sets the IPSec VPN Connection Capability Status to unknown
conn-cap esp closed	Sets the ESP Connection Capability Status to clsoed
conn-cap esp open	Sets the ESP Connection Capability Status to open
conn-cap esp unknown	Sets the ESP Connection Capability Status to unknown
custm-conn-cap <NUMBER> ip-proto <NUMBER> port <NUMBER> status closed	Sets Status to closed.
custm-conn-cap <NUMBER> ip-proto <NUMBER> port <NUMBER> status closed description <WORD>	Sets the description of Connection Capability entry.
custm-conn-cap <NUMBER> ip-proto <NUMBER> port <NUMBER> status open	Sets Status to open.
custm-conn-cap <NUMBER> ip-proto <NUMBER> port <NUMBER> status open description <WORD>	Sets the description of Connection Capability entry.

custm-conn-cap <NUMBER> ip-proto <NUMBER> port <NUMBER> status unknown	Sets Status to unknown.
custm-conn-cap <NUMBER> ip-proto <NUMBER> port <NUMBER> status unknown description <WORD>	Sets the description of Connection Capability entry.
adv-gas cb-delay <NUMBER>	Sets the GAS Comeback Delay.
adv-gas rsp-limit <NUMBER>	Sets the GAS query response length limit.
adv-gas rsp-buf-time <NUMBER>	Sets the GAS query response buffering time.
adv-gas dos-detect	Enables the GAS DOS detection.
adv-gas dos-maxreq <NUMBER>	Set the GAS DOS detection maximum request number.
hs-caps operating-class-indication 2.4	Sets the operating class indication to 2.4 GHz.
hs-caps operating-class-indication 5	Sets the operating class indication to 5 GHz.
hs-caps operating-class-indication dual-band	Sets the operating class indication to 2.4/5 GHz.
show	Displays hotspot 2.0 operator settings.

hs20sp

Use the following command to configure a Hotspot 2.0 Service Provider entry:

```
hs20sp <WORD>
```

Example

ruckus(config)# **hs20sp serviceprovider1**

The Hotspot (2.0) service provider entry 'serviceprovider1' has been created.

ruckus(config-hs20sp)# **end**

The Hotspot (2.0) service provider entry has saved successfully.

Your changes have been saved.

```
ruckus(config)#
```

no hs20sp

Use the following command to delete a Hotspot 2.0 Service Provider entry:

```
no hs20sp <WORD>
```

Example

```
ruckus(config)# no hs20sp provider1
The Hotspot (2.0) service provider 'provider1' has been deleted.
ruckus(config)#
```

Configure Hotspot 2.0 Service Provider Settings

The following commands can be used to configure Hotspot 2.0 Service Provider entry settings. To execute these commands, you must first create or edit a Hotspot 2.0 Service Provider entry using the `hs20sp` command and entering the `config-hs20sp` context.

Syntax Description

help	Shows available commands.
history	Shows a list of previously run commands.
abort	Exits the config-hs20sp context without saving changes.
end	Saves changes, and then exits the config-hs20sp context.
exit	Saves changes, and then exits the config-hs20sp context.
quit	Exits the config-hs20sp context without saving changes.
no nai-realm <NUMBER>	Deletes a NAI Realm entry.
no domain-name <NUMBER>	Deletes a domain name entry.
no roam-consortium <NUMBER>	Deletes a roaming consortium entry.
no anqp-3gpp-info <NUMBER>	Deletes a 3GPP cellular network information entry.
name <WORD>	Sets the hotspot(2.0) service provider entry name.
description <WORD>	Sets the hotspot(2.0) service provider entry description.
nai-realm <NUMBER>	Creates a new NAI Realm entry or modifies an existing entry.

domain-name <NUMBER>	Creates a new domain name entry or modifies an existing entry.
domain-name <NUMBER> name <WORD>	Sets the domain name of a domain name entry.
roam-consortium <NUMBER>	Creates a new roaming consortium entry or modifies an existing entry.
roam-consortium <NUMBER> org-id <HEX>	Sets the organization ID of a roaming consortium entry.
roam-consortium <NUMBER> org-id <HEX> name <WORD>	Sets the name of a roaming consortium entry.
anqp-3gpp-info <NUMBER>	Creates a 3GPP cellular network information entry or modifies an existing entry list.
anqp-3gpp-info <NUMBER> mcc <NUMBER>	Sets the MCC of 3GPP cellular network information entry.
anqp-3gpp-info <NUMBER> mcc <NUMBER> mnc <NUMBER>	Sets the MNC of 3GPP cellular network information entry.
anqp-3gpp-info <NUMBER> mcc <NUMBER> mnc <NUMBER> name <WORD>	Sets the name of 3GPP cellular network information entry.
show	Displays hotspot 2.0 service provider settings.

nai-realm

To create, a new NAI Realm entry or modifies an existing entry, use the following command:

```
nai-realm <NUMBER>
```

This command enters the config-hs20sp-nai-realm context. The following commands can be executed from within this context.

Syntax Description

name	Sets the name of the NAI Realm entry.
encoding	Sets the encoding of the NAI Realm entry.
eap-method <NUMBER>	Sets the EAP method #X of the NAI Realm entry. (X:1~4)
no	Contains commands that can be executed from within the context.
show	Displays NAI Realm settings.

Example

```
ruckus(config-hs20sp)# nai-realm 1
ruckus(config-hs20sp-nai-realm)# name realm1
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-hs20sp-nai-realm)# show
          Name= realm1
          Encoding= RFC-4282
          EAP Method #1= N/A
          EAP Method #2= N/A
          EAP Method #3= N/A
          EAP Method #4= N/A
ruckus(config-hs20sp-nai-realm)# end
To save the changes, type 'end' or 'exit'.
ruckus(config-hs20sp)# end
The Hotspot (2.0) service provider entry has saved successfully.
Your changes have been saved.
ruckus(config)#
```

name

Use the following command to set the name of the NAI Realm entry:

```
name <WORD>
```

encoding

Use the following command to set the encoding of the NAI Realm entry:

```
encoding [rfc-4282 | utf-8]
```

eap-method

Use the following command to set the EAP method of the NAI Realm entry:

```
eap-method <NUMBER>
```

eap-method eap-mthd

Use the following command to set the EAP method of the NAI Realm entry:

```
eap-method <NUMBER> eap-mthd [N/A | <NAME>]
```

Syntax Description

N/A	Sets the EAP method of the NAI Realm entry to N/A.

MD5-Challenge	Sets the EAP method of the NAI Realm entry to MD5-Challenge.
EAP-TLS	Sets the EAP method of the NAI Realm entry to EAP-TLS.
EAP-CISCO	Sets the EAP method of the NAI Realm entry to EAP-Cisco.
EAP-SIM	Sets the EAP method of the NAI Realm entry to EAP-SIM.
EAP-TTLS	Sets the EAP method of the NAI Realm entry to EAP-SIM.
PEAP	Sets the EAP method of the NAI Realm entry to PEAP.
MSCHAP-V2	Sets the EAP method of the NAI Realm entry to EAP-MSCHAP-V2.
EAP-AKA	Sets the EAP method of the NAI Realm entry to EAP-AKA.
EAP-AKA-Prime	Sets the EAP method of the NAI Realm entry to EAP-AKA'.
Reserved	Sets the EAP method of the NAI Realm entry to Reserved.

Syntax Description

```
ruckus(config-hs20sp-nai-realm)# eap-method 1 eap-mthd EAP-TLS
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-hs20sp-nai-realm)#
```

eap-method auth-info

To set the Auth Info of the EAP method, use the following command:

```
eap-method <NUMBER> auth-info <NUMBER>
```

Syntax Description

auth-id	Sets the auth info ID of the auth info.
auth-id expanded-EAP-method	Sets the Auth Info of the EAP method to expanded-EAP-method.
auth-id expanded-EAP-method vndr-id <NUMBER>	Sets the vendor ID of the auth info.
auth-id expanded-EAP-method vndr-id <NUMBER> vndr-type <NUMBER>	Sets the vendor type of the auth info.

auth-id nonEAP-inner-auth	Sets the Auth Info of the EAP method to Non-EAP Inner Authentication Type.
auth-id nonEAP-inner-auth auth-type	Sets the auth info type of the auth info.
auth-id nonEAP-inner-auth auth-type Reserved	Sets the Non-EAP Inner Authentication Type to Reserved.
auth-id nonEAP-inner-auth auth-type PAP	Sets the Non-EAP Inner Authentication Type to PAP.
auth-id nonEAP-inner-auth auth-type CHAP	Sets the Non-EAP Inner Authentication Type to CHAP.
auth-id nonEAP-inner-auth auth-type MSCHAP	Sets the Non-EAP Inner Authentication Type to MSCHAP.
auth-id nonEAP-inner-auth auth-type MSCHAPV2	Sets the Non-EAP Inner Authentication Type to MSCHAPV2.
auth-id inner-auth-EAP-mthd	Sets the Auth Info of the EAP method to Inner Authentication EAP Method Type.
auth-id inner-auth-EAP-mthd auth-type	Sets the auth info type of the auth info.
auth-id inner-auth-EAP-mthd auth-type EAP-TLS	Sets the Inner Authentication EAP Method Type to EAP-TLS.
auth-id inner-auth-EAP-mthd auth-type EAP-SIM	Sets the Inner Authentication EAP Method Type to EAP-SIM.
auth-id inner-auth-EAP-mthd auth-type EAP-TTLS	Sets the Inner Authentication EAP Method Type to EAP-TTLS.
auth-id inner-auth-EAP-mthd auth-type EAP-AKA	Sets the Inner Authentication EAP Method Type to EAP-AKA.
auth-id inner-auth-EAP-mthd auth-type EAP-AKA-Prime	Sets the Inner Authentication EAP Method Type to EAP-AKA'.
auth-id exp-inner-EAP-mthd	Sets the Auth Info of the EAP method to expanded-inner-EAP-method.
auth-id exp-inner-EAP-mthd vndr-id <NUMBER>	Sets the vendor ID of the auth info.
auth-id exp-inner-EAP-mthd vndr-id <NUMBER> vndr-type <NUMBER>	Sets the vendor type of the auth info.
auth-id credential-type	Sets the Auth Info of the EAP method to Credential Type.
auth-id credential-type auth-type	Sets the auth info type of the auth info.

auth-id credential-type auth-type SIM	Sets the Credential Type to SIM.
auth-id credential-type auth-type USIM	Sets the Credential Type to USIM.
auth-id credential-type auth-type NFC-secure-elem	Sets the Credential Type to NFC Secure Element.
auth-id credential-type auth-type hardware-token	Sets the Credential Type to Hardware Token.
auth-id credential-type auth-type softoken	Sets the Credential Type to Softoken.
auth-id credential-type auth-type certificate	Sets the Credential Type to Certificate.
auth-id credential-type auth-type username-password	Sets the Credential Type to username/password.
auth-id credential-type auth-type none	Sets the Credential Type to none.
auth-id credential-type auth-type reserved	Sets the Credential Type to Reserved.
auth-id tunnel-EAP-mthd-crdn-type	Sets the Auth Info of the EAP method to Tunneled EAP Method Credential Type.
auth-id tunnel-EAP-mthd-crdn-type auth-type	Sets the auth info type of the auth info.
auth-id tunnel-EAP-mthd-crdn-type auth-type SIM	Sets the Tunneled EAP Method Credential Type to SIM.
auth-id tunnel-EAP-mthd-crdn-type auth-type USIM	Sets the Tunneled EAP Method Credential Type to USIM.
auth-id tunnel-EAP-mthd-crdn-type auth-type NFC-secure-elem	Sets the Tunneled EAP Method Credential Type to NFC Secure Element.
auth-id tunnel-EAP-mthd-crdn-type auth-type hardware-token	Sets the Tunneled EAP Method Credential Type to Hardware Token.
auth-id tunnel-EAP-mthd-crdn-type auth-type softoken	Sets the Tunneled EAP Method Credential Type to Softoken.
auth-id tunnel-EAP-mthd-crdn-type auth-type certificate	Sets the Tunneled EAP Method Credential Type to Certificate.
auth-id tunnel-EAP-mthd-crdn-type auth-type username-password	Sets the Tunneled EAP Method Credential Type to username/password.
auth-id tunnel-EAP-mthd-crdn-type auth-type reserved	Sets the Tunneled EAP Method Credential Type to Reserved.

auth-id tunnel-EAP-mthd-crdn-type auth-type anonymous	Sets the Tunneled EAP Method Credential Type to Anonymous.
no eap-method <NUMBER>	Sets the EAP method #X of the NAI Realm entry. (X:1~4)
no eap-method <NUMBER> auth-info <NUMBER>	Disable the Auth Info of the EAP method
show	Displays NAI Realm settings.

Configure Mesh Commands

Use the `mesh` commands to configure the controller's mesh networking settings. To run these commands, you must first enter the `config-mesh` context.

mesh

Use the `mesh` command to enter the config-mesh context and configure the mesh-related settings.

```
mesh
```

Syntax Description

`mesh`	Configure mesh settings

Defaults

none

Example

```
ruckus(config)# mesh
ruckus(config-mesh)#
```

abort

To exit the `config-mesh` context without saving changes, use the `abort` command.

```
abort
```

Syntax Description

abort	Exit the mesh settings without saving changes

Defaults

None.

Example

```
ruckus(config-mesh)# abort
No changes have been saved.
ruckus(config)#
```

end

To save changes, and then exit the `config-mesh` context, use the following command:

```
end
```

Syntax Description

end	Save changes, and then exit the context

Defaults None.

Example

```
ruckus(config-mesh)# end
Are you sure you want to enable mesh[Y/n]
Your changes have been saved.
ruckus(config)#
```

exit

To save changes, and then exit the `config-mesh` context, use the following command:

```
exit
```

Syntax Description

exit	Save changes, and then exit the context

Defaults None.

Example

```
ruckus(config-mesh)# exit
Are you sure you want to enable mesh[Y/n]
Your changes have been saved.
ruckus(config)#
```

quit

To exit the `config-mesh` context without saving changes, use the `quit` command.

```
quit
```

Syntax Description

quit	Exit the mesh settings without saving changes

Defaults None.

Example

```
ruckus(config-mesh)# quit
No changes have been saved.
ruckus(config)#
```

show

To display the current mesh settings, use the following command:

```
show
```

Syntax Description

show	Display the current mesh settings

Defaults

None.

Example

```
ruckus(config-mesh)# show
Mesh Settings:
Mesh Status= Enabled
Mesh Name(ESSID)= Mesh-000000000311
Mesh Passphrase= GdxW5CUgNn_SEHOPyCSxv_chHSca MH-OpnRGfX sRvwXBJL-
wUsD64eK8CMEZfm
Mesh Hop Detection:
Status= Disabled
Mesh Downlinks Detection:
Status= Disabled
Tx. Rate of Management Frame=2Mbps
Beacon Interval= 200ms
ruckus(config-mesh)#
```

ssid

To set the SSID of the mesh network, use the following command:

```
ssid <WORD/SSID>
```

Syntax Description

ssid	Set the SSID of the mesh network
<WORD/SSID>	Set to this SSID

Defaults

None.

Example

```
ruckus(config-mesh)# ssid rks_mesh
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

passphrase

To set the passphrase that allows access to the mesh network, use the following command:

```
passphrase <WORD>
```

Syntax Description

passphrase	Set the passphrase that allows access to the mesh network
<WORD>	Set to this passphrase

Defaults

None.

Example

```
ruckus(config-mesh)# passphrase test123456
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

hops-warn-threshold

To enable and configure the mesh hop threshold, use the following command:

```
hops-warn-threshold <NUMBER>
```

Syntax Description

hops-warn-threshold	Set the mesh hop threshold (max hops)
<NUMBER>	Set to this threshold value

Defaults

5

Example

```
ruckus(config-mesh)# hops-warn-threshold 6
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

no detect-hops

To disable the mesh hop threshold, use the following command:

```
no detect-hops
```

Syntax Description

no detect-hops	Disable the mesh hop threshold

Defaults

None.

Example

```
ruckus(config-mesh)# no detect-hops
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

fan-out-threshold

To enable and configure the mesh downlink threshold, use the following command:

```
fan-out-threshold <NUMBER>
```

Syntax Description

fan-out-threshold	Set the mesh downlink threshold (max downlinks)
<NUMBER>	Set to this threshold value

Defaults

5

Example

```
ruckus(config-mesh)# fan-out-threshold 8
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

no detect-fanout

To disable the mesh downlink threshold, use the following command:

```
no detect-fanout
```

Syntax Description

no detect-fanout	Disable the mesh downlink threshold

Defaults

None.

Example

```
ruckus(config-mesh)# no detect-fanout
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

beacon-interval

To set the beacon interval for mesh links, use the following command:

```
beacon-interval <NUMBER>
```

Syntax Description

beacon-interval	Set the beacon interval for mesh links
<NUMBER>	Enter the beacon interval (100~1000 TUs)

Defaults

200

Example

```
ruckus(config-mesh)# beacon-interval 200
```

```
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-mesh)#
```

mgmt-tx-rate

To set the transmit rate for management frames, use the following command:

mgmt-tx-rate <RATE>

Syntax Description

mgmt-tx-rate	Set the max transmit rate for management frames
<RATE>	Set the transmit rate (in Mbps).

Defaults

2

Example

```
ruckus(config-mesh)# mgmt-tx-rate 2
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-mesh)#
```

Configure Alarm Commands

Use the `alarm` commands to configure the controller's alarm notification settings. To run these commands, you must first enter the `config-alarm` context.

alarm

To enter the `config-alarm` context, use the following command.

```
alarm
```

Example

```
ruckus(config)# alarm
ruckus(config-alarm)#
```

no alarm

To disable alarm settings, use the following command:

```
no alarm
```

Example

```
ruckus(config)# no alarm
The Alarm settings have been updated.
```

```
ruckus(config)#
```

abort

To exit the `config-alarm` context without saving changes, use the `abort` command.

```
abort
```

Syntax Description

abort	Exit the alarm settings without saving changes

Defaults

None.

Example

```
ruckus(config-alarm)# abort
No changes have been saved.
ruckus(config)#
```

end

To save changes, and then exit the `config-alarm` context, use the following command:

```
end
```

Syntax Description

end	Save changes, and then exit the context

Defaults

None.

Example

```
ruckus(config-alarm)# end
The Alarm settings have been updated.
Your changes have been saved.
ruckus(config)#
```

exit

To save changes, and then exit the `config-alarm` context, use the following command:

```
exit
```

Syntax Description

exit	Save changes, and then exit the context

Defaults None.

Example

```
ruckus(config-alarm)# exit
The Alarm settings have been updated.
Your changes have been saved.
```

quit

To exit the `config-alarm` context without saving changes, use the `quit` command.

```
quit
```

Syntax Description

quit	Exit the alarm settings without saving changes

Defaults None.

Example

```
ruckus(config-alarm)# quit
No changes have been saved.
ruckus(config)#
```

show

To display the current alarm settings, use the following command:

```
show
```

Syntax Description

show	Display the current alarm settings

Defaults None.

Example

```
rruckus(config)# alarm
ruckus(config-alarm)# show
Alarm:
  Status= Enabled
  Email Address= johndoe@gmail.com
  E-mail From = zonedirector@ruckuswireless.com
  SMTP Server Name= smtp.gmail.com
  SMTP Server Port= 587
  SMTP Authentication Username= johndoe@gmail.com
  SMTP Authentication Password= ***********
  wait time=
```

```
  SMTP Encryption Options:
    TLS= Enabled
    STARTTLS= Enabled

ruckus(config-alarm)#
```

e-mail

To set the email address to which alarm notifications will be sent, use the following command:

```
e-mail <WORD>
```

Syntax Description

e-mail	Set the email address to which alarm notifications will be sent
<WORD>	Send alarm notifications to this email address

Defaults

None.

Example

```
ruckus(config-alarm)# e-mail joe@163.com
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

from

To set the sender from address for email alarms, use the following command:

```
from <WORD>
```

Syntax Description

from	Set the email address from which alarm notifications will be sent
<WORD>	Send alarm notifications from this email address

Defaults

None.

Example

```
ruckus(config-alarm)# from zonedirector@zonedirector.com
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-alarm)#
```

smtp-server-name

To set the SMTP server that ZoneDirector uses to send alarm notifications, use the following command:

```
smtp-server-name <WORD>
```

Syntax Description

smtp-server-name	Set the SMTP server that ZoneDirector uses to send alarm notifications
<WORD>	Set to this SMTP server name

Defaults

None.

Example

```
ruckus(config-alarm)# smtp-server-name smtp.163.com
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

smtp-server-port

To set the SMTP server port that ZoneDirector uses to send alarm notifications, use the following command:

```
smtp-server-port <NUMBER>
```

Syntax Description

smtp-server-port	Set the SMTP server port that ZoneDirector uses to send alarm notifications
<NUMBER>	Set to this SMTP server port

Defaults

587

Example

```
ruckus(config-alarm)# smtp-server-port 25
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

smtp-auth-name

To set the user name that ZoneDirector uses to authenticate with the SMTP server,use the following command:

```
smtp_auth_name <WORD>
```

Syntax Description

smtp_auth_name	Set the user name that ZoneDirector uses to authenticate with the SMTP server

<WORD>	Set to this user name

Defaults

None.

Example

```
ruckus(config-alarm)# smtp-auth-name joe
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

smtp-auth-password

To set the password that ZoneDirector uses to authenticate with the SMTP server,use the following command:

```
smtp-auth-password <WORD>
```

Syntax Description

smtp-auth-password	Set the password that ZoneDirector uses to authenticate with the SMTP server
<WORD>	Set to this password

Defaults

None.

Example

```
ruckus(config-alarm)# smtp-auth-password 123456
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

smtp-wait-time

To set the SMTP server wait time (in seconds), use following command:

```
smtp-wait-time <NUMBER>
```

Example

```
ruckus(config-alarm)# smtp-wait-time 10
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-alarm)#
```

tls-smtp-encryption

To enable TLS for SMTP encryption of alarm notifications, use the following command:

```
tls-smtp-encryption [tls|starttls]
```

Syntax Description

tls-smtp-encryption	Enable SMTP encryption of alarm notifications

tls	Enable TLS encryption for alarm notifications
starttls	Enable STARTTLS encryption for alarm notifications

Defaults

None.

Example

```
ruckus(config-alarm)# tls-smtp-encryption tls
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

no tls-smtp-encryption

To disable TLS for SMTP encryption of alarm notifications, use the following command:

```
no tls-smtp-encryption [tls | starttls]
```

Syntax Description

no tls-smtp-encryption	Disable SMTP encryption of alarm notifications
tls	Disable TLS encryption
starttls	Disable STARTTLS encryption

Defaults

None.

Example

```
ruckus(config-alarm)# no tls-smtp-encryption tls
The command was executed successfully. To save the changes, type
'end' or 'exit'.
```

Configure Alarm-Event Settings

Use the alarm-event command to configure which events will trigger ZoneDirector email alerts. Entering this command enters the config-alarm-event context.

alarm-event

To enable email alarm notifications for specific event types, use the following command:

```
alarm-event
```

Syntax Description

event all	Enable email alarms for all event types
no event all	Disable email alarms for all event types

event rogue-ap-detected	Enable email notification when Rogue AP detected
event rogue-device-detected	Enable email notification when Ad hoc network detected
event ap-lost-contacted	AP lost contact
event ssid-spoofing-ap-detected	SSID spoofing AP detected
event mac-spoofing-ap-detected	MAC spoofing AP detected
event rogue-dhcp-server-detected	Rogue DHCP server detected
event temporary-license-expired	Temporary license has expired
event temporary-license-will-expire	Temporary license will expire
event lan-rogue-ap-detected	LAN Rogue AP detected
event aaa-server-unreachable	AAA server unreachable
event ap-has-hardware-problem	AP hardware problem detected
event uplink-ap-lost	Mesh AP uplink connection lost
event incomplete-primary/secondary-ip-settings	AP fails to maintain primary/secondary ZD IP address settings
event smart-redundancy-state-changed	Smart Redundancy device status change detected
event smart-redundancy-active-connected	Smart Redundancy device active device connected
event smart-redundancy-standby-connected	Smart Redundancy standby device connected
event smart-redundancy-active-disconnected	Smart Redundancy active device disconnected
event smart-redundancy-standby-disconnected	Smart Redundancy standby device disconnected
test-alarm ap-lose-connection	Test AP connection lost alarm event
show	Show alarm settings

Defaults

All enabled

Example

```
ruckus(config-alarm)# no event all
ruckus(config-alarm)# event uplink-ap-lost
ruckus(config-alarm)# show
Alarm:
Status= Enabled
Email Address= johndoe@gmail.com
```

```
E-mail From = zonedirector@ruckuswireless.com
SMTP Server Name= smtp.gmail.com
SMTP Server Port= 25
SMTP Authentication Username= johndoe@gmail.com
SMTP Authentication Password= test123
wait time=
SMTP Encryption Options:
TLS= Enabled
STARTTLS= Enabled
Alarm Events Notify By Email:
MSG_rogue_AP_detected= disabled
MSG_ad_hoc_network_detected= disabled
MSG_AP_lost= disabled
MSG_SSID_spoofing_AP_detected= disabled
MSG_MAC_spoofing_AP_detected=disabled
MSG_admin_rogue_dhcp_server= disabled
MSG_admin_templic_oneday=disabled
MSG_lanrogue_AP_detected=disabled
MSG_RADIUS_service_outage= disabled
MSG_AP_hardware_problem= disabled
MSG_ZD_Sensor_problem= disabled
MSG_AP_no_mesh_uplink= enabled
MSG_AP_keep_no_AC_cfg= disabled
MSG_cltr_change_to_active= disabled
MSG_cltr_active_connected= disabled
MSG_cltr_standby_connected=disabled
MSG_cltr_active_disconnected=disabled
MSG_cltr_standby_disconnected= disabled

ruckus(config-alarm)#
```

no event

To disable email alarm notifications for specific event types, use the following command:

```
no event <event_name>
```

Syntax Description

no event	Disable email alarms for this event type
all	Disable email alarms for all event types
rogue-ap-detected	Rogue AP detected

rogue-device-detectedq	Ad hoc network detected
ap-lost-contacted	AP lost contact
ssid-spoofing-ap-detected	SSID spoofing AP detected
mac-spoofing-ap-detected	MAC spoofing AP detected
rogue-dhcp-server-detected	Rogue DHCP server detected
temporary-license-expired	Temporary license has expired
temporary-license-will-expire	Temporary license will expire
lan-rogue-ap-detected	LAN Rogue AP detected
aaa-server-unreachable	AAA server unreachable
ap-has-hardware-problem	AP hardware problem detected
uplink-ap-lost	Mesh AP uplink connection lost
incomplete-primary/secondary-ip-settings	AP fails to maintain primary/secondary ZD IP address settings
smart-redundancy-state-changed	Smart Redundancy device status change detected
smart-redundancy-active-connected	Smart Redundancy device active device connected
smart-redundancy-standby-connected	Smart Redundancy standby device connected
smart-redundancy-active-disconnected	Smart Redundancy active device disconnected
smart-redundancy-standby-disconnected	Smart Redundancy standby device disconnected

Configure Services Commands

Use the `services` commands to configure miscellaneous service settings, such as automatic power and channel selection settings, ChannelFly, background scanning, rogue AP and rogue DHCP server detection, etc. To run these commands, you must first enter the `config-services` context.

abort

To exit the `config-services` context without saving changes, use the `abort` command.

```
abort
```

Syntax Description

abort	Exit the service settings without saving changes

Defaults None.

Example

```
ruckus(config-services)# abort
No changes have been saved.
ruckus(config)#
```

end

To save changes, and then exit the `config-services` context, use the following command:

```
end
```

Syntax Description

end	Save changes, and then exit the context

Defaults None.

Example

```
ruckus(config-services)# end
Your changes have been saved.
ruckus(config)#
```

exit

To save changes, and then exit the `config-services` context, use the following command:

```
exit
```

Syntax Description

exit	Save changes, and then exit the context

Defaults None.

Example

```
ruckus(config-services)# exit
Your changes have been saved.
ruckus(config)#
```

quit

To exit the `config-services` context without saving changes, use the `quit` command.

```
quit
```

Syntax Description

quit	Exit the service settings without saving changes

Defaults None.

Example

```
ruckus(config-services)# quit
No changes have been saved.
ruckus(config)#
```

auto-adjust-ap-power

To enable the auto adjustment of theAP radio power, which helps optimize radio coverage when radio interference is present, use the following command:

```
auto-adjust-ap-power
```

Syntax Description

auto-adjust-ap-power	Enable the auto adjustment of theAP radio power

Defaults None.

Example

```
ruckus(config-services)# auto-adjust-ap-power
The command was executed successfully.
```

no auto-adjust-ap-power

To disable the auto adjustment of theAP radio power, which helps optimize radio coverage when radio interference is present, use the following command:

```
no auto-adjust-ap-power
```

Syntax Description

no auto-adjust-ap-power	Disable the auto adjustment of theAP radio power

Defaults None.

Example

```
ruckus(config-services)# no auto-adjust-ap-power
The command was executed successfully.
```

auto-adjust-ap-channel

To enable the auto adjustment of theAP radio channel when radio interference is present, use the following command:

```
auto-adjust-ap-channel
```

Syntax Description

auto-adjust-ap-channel	Enable the auto adjustment of theAP radio channel

Defaults

None.

Example

```
ruckus(config-services)# auto-adjust-ap-channel
The command was executed successfully.
```

no auto-adjust-ap-channel

To disable the auto adjustment of theAP radio channel when radio interference is present, use the following command:

```
no auto-adjust-ap-channel
```

Syntax Description

no auto-adjust-ap-channel	Disable the auto adjustment of theAP radio channel

Defaults

None.

Example

```
ruckus(config-services)# no auto-adjust-ap-channel
The command was executed successfully.
```

channelfly

To enable ChannelFly channel management, use the following command:

```
channelfly [radio-2.4-mtbc | radio-5-mtbc] <NUMBER>
```

Syntax Description

channelfly	Enable ChannelFly automatic adjustment of theAP radio channel
radio-2.4	Enable ChannelFly on the 2.4 GHz radio
radio-5	Enable ChannelFly on the 5 GHz radio
mtbc	Set the mean time between channel changes
<NUMBER>	Number in minutes (1~1440) to set as mean time between channel change

Defaults

Enabled for both 2.4 and 5 GHz radios

MTBC: 100

Example

```
ruckus(config-services)# channelfly radio-2.4 100
The command was executed successfully.
ruckus(config-services)#
```

Example

```
ruckus(config-services)# channelfly radio-2.4-mtbc 100
The command was executed successfully.
ruckus(config-services)#
```

no channelfly

To disable ChannelFly channel management, use the following command:

```
no channelfly [radio-2.4 | radio-5]
```

Syntax Description

no channelfly	Disable ChannelFly automatic adjustment of theAP radio channel
radio-2.4	Disable ChannelFly on the 2.4 GHz radio
radio-5	Disable ChannelFly on the 5 GHz radio

Defaults

None.

Example

```
ruckus(config-services)# no channelfly radio-2.4
The command was executed successfully.
ruckus(config-services)# no channelfly radio-5
The command was executed successfully.
ruckus(config-services)#
```

background-scan

To enable background scanning and configure the scan interval, use the following command:

```
background-scan [radio-2.4-interval | radio-5-interval]
<NUMBER>
```

Syntax Description

background-scan	Enable background scanning and configure the scan interval
radio-2.4-interval	Configure background scanning interval for the 2.4 GHz radio
radio-5-interval	Configure background scanning interval for theGHz radio

<NUMBER>	Perform background scan at this interval (in seconds)

Defaults

20 seconds

Example

```
ruckus(config-services)# background-scan radio-2.4-interval 6
The command was executed successfully.
```

no background-scan

To disable background scanning on the 2.4GHz radio, use the following command:

```
no background-scan [radio-2.4|radio-5]
```

Syntax Description

no background-scan	Disable background scanning
radio-2.4	Disable background scanning on the 2.4GHz radio
radio-5	Disable background scanning on the 5GHz radio

Defaults

None

Example

```
ruckus(config-services)# no background-scan radio-2.4
The command was executed successfully.
ruckus(config-services)# no background-scan radio-5
The command was executed successfully.
```

aeroscout-detection

To enable detection of AeroScout RFID Tags by APs that are managed by ZoneDirertor, use the following command:

```
aeroscout-detection
```

Syntax Description

aeroscout-detection	Enable detection of AeroScout RFID Tags by APs

Defaults

None

Example

```
ruckus(config-services)# aeroscout-detection
The command was executed successfully.
```

no aeroscout-detection

To disable detection of AeroScout RFID Tags by APs that are managed by ZoneDirertor, use the following command:

```
no aeroscout-detection
```

Syntax Description

no aeroscout-detection	Disable detection of AeroScout RFID Tags by APs

Defaults None

Example

```
ruckus(config-services)# no aeroscout-detection
The command was executed successfully.
```

tun-encrypt

To enable tunnel encryption for tunneled traffic, use the following command:

```
tun-encrypt
```

Defaults Disabled

Example

```
ruckus(config-services)# tun-encrypt
The command was executed successfully.
```

no tun-encrypt

To disable tunnel encryption for tunneled traffic, use the following command:

```
no tun-encrypt
```

Defaults Disabled

Example

```
ruckus(config-services)# no tun-encrypt
The command was executed successfully.
```

tun-block-mcast all

To enable multicast blocking for tunneled traffic, use the following command:

```
tun-block-mcast all
```

Defaults Disabled

Example

```
ruckus(config-services)# tun-block-mcast all
The command was executed successfully.
ruckus(config-services)#
```

tun-block-mcast non-well-known

To enable multicast blocking for non-well-known tunneled traffic, use the following command:

```
tun-block-mcast non-well-known
```

Defaults

Disabled

Example

```
ruckus(config-services)# tun-block-mcast non-well-known
The command was executed successfully.
ruckus(config-services)#
```

no tun-block-mcast

To disable blocking multicast traffic from network to tunnel, use the following command:

```
no tun-block-mcast
```

tun-block-bcast

To enable broadcast blocking for tunneled traffic, use the following command:

```
tun-block-bcast
```

Defaults

Disabled

Example

```
ruckus(config-services)# tun-block-bcast
The command was executed successfully.
ruckus(config-services)#
```

no tun-block-bcast

To disables blocking broadcast traffic from network to tunnel except ARP and DHCP, use the following command:

```
no tun-block-bcast
```

tun-proxy-arp

To enable proxy ARP service for tunneled traffic, use the following command:

```
tun-proxy-arp <NUMBER>
```

Defaults

Disabled

Example

```
ruckus(config-services)# tun-proxy-arp 1000
The command was executed successfully.
ruckus(config-services)#
```

no tun-proxy-arp

To disable Proxy ARP for the tunneled WLAN, use the following command:

```
no tun-proxy-arp
```

tun-ip-ageing

To set ageing time for IP/IPv6 table, use the following command:

```
tun-ip-ageing <NUMBER>
```

pif

To enable Packet Inspection Filter and set rate limiting threshold, use the following command:

```
pif [uplink-proc | rate-limit <NUMBER>]
```

Syntax Description

pif	Enable Packet Inspection Filter
uplink-proc	Enable uplink process of Packet Inspection Filter
rate-limit	Enable and set Broadcast Neighbor Discovery Packets (ARP and ICMPv6 Neighbor Solicit) rate limit threshold.
<NUMBER>	Rate limiting threshold for PIF feature.

Example

```
ruckus(config-services)# pif uplink-proc
The command was executed successfully.
ruckus(config-services)# pif rate-limit 1000
The command was executed successfully.
ruckus(config-services)# show
Services:
  Automatically adjust ap radio power= Disabled
  Automatically adjust ap channel= Enabled
  Channelfly works on 2.4GHz radio:
    Status= Disabled
  Channelfly works on 5GHz radio:
    Status= Disabled
```

```
  Run a background scan on 2.4GHz radio:
    Status= Enabled
    Time= 20 seconds
  Run a background scan on 5GHz radio:
    Status= Enabled
    Time= 20 seconds
  AeroScout RFID tag detection= Disabled
  Tunnel encryption for tunneled traffic= Enabled
  Block multicast traffic from network to tunnel= Disabled
  Block broadcast traffic from network to tunnel except ARP and
DHCP= Disabled
  Tunnel Proxy ARP of tunnel WLAN:
    status= Disabled
  Packet Inspection Filter(PIF) uplink process= Enabled
  Packet Inspection Filter(PIF) rate limit:
    status= Enabled
    rate limit= 1000
ruckus(config-services)#
```

no pif

To disable uplink process of packet inspection filter or disables Broadcast Neighbor Discovery Packets (ARP and ICMPv6 Neighbor Solicit), use the following command:

```
no pif [uplink-proc | rate-limit <NUMBER>]
```

show

To display the current service settings, use the following command:

```
show
```

Syntax Description

show	Display the current service settings

Defaults

None.

Example

```
ruckus(config-services)# show
Services:
  Automatically adjust ap radio power= Disabled
  Automatically adjust ap channel= Enabled
  Channelfly works on 2.4GHz radio:
    Status= Disabled
  Channelfly works on 5GHz radio:
    Status= Disabled
```

```
  Run a background scan on 2.4GHz radio:
    Status= Enabled
    Time= 2000 seconds
  Run a background scan on 5GHz radio:
    Status= Enabled
    Time= 2000 seconds
  AeroScout RFID tag detection= Disabled
  Tunnel encryption for tunneled traffic= Disabled
  Block multicast traffic from network to tunnel= Block non well-
known
  Block broadcast traffic from network to tunnel except ARP and
DHCP= Disabled
  Tunnel Proxy ARP of tunnel WLAN:
    status= Disabled
    ageing time= 0
  Packet Inspection Filter(PIF) uplink process= Disabled
  Packet Inspection Filter(PIF) rate limit:
    status= Disabled
ruckus(config-services)#
```

Configure WIPS Commands

Use the `wips` commands to configure Wireless Intrusion Prevention settings. To run these commands, you must first enter the `config-wips` context.

wips

Use the `wips` command to enter the config-wips context and configure WIPS settings.

```
wips
```

Syntax Description

help	Shows available commands.
history	Shows a list of previously run commands.
end	Saves changes, and the exits the config-wips context.
exit	Saves changes, and the exits the config-wips context.
no	Disable WIPS services.
protect-excessive-wireless-request	Enables protecting the wireless network against excessive wireless requests.

temp-block-auth-failed-client	Temporarily block wireless clients with repeated authentication failures.
rogue-report	Enables report rogue devices in ZD event log.
malicious-report	Enables protecting the network from malicious rogue access points.
rogue-dhcp-detection	Enables rogue DHCP server detection.
show	Displays the WIPS settings.

Example

```
ruckus(config)# wips
ruckus(config-wips)# show
  Protect my wireless network against excessive wireless requests= Disabled
  Temporarily block wireless clients with repeated authentication failures:
    Status= Enabled
    Time= 30 seconds
  Report rogue devices in ZD event log= Enabled
  Protect the network from malicious rogue access points= Disabled
  Rogue DHCP server detection= Enabled
ruckus(config-wips)# temp-block-auth-failed-client time 45
The command was executed successfully.
ruckus(config-wips)# show
  Protect my wireless network against excessive wireless requests= Disabled
  Temporarily block wireless clients with repeated authentication failures:
    Status= Enabled
    Time= 45 seconds
  Report rogue devices in ZD event log= Enabled
  Protect the network from malicious rogue access points= Disabled
  Rogue DHCP server detection= Enabled
ruckus(config-wips)# end
Your changes have been saved.
ruckus(config)#
```

4

Using Debug Commands

In This Chapter

Debug Commands Overview

This section describes the commands that you can use to debug ZoneDirector and connected APs, and to configure debug log settings. From the privileged commands context, type **debug** to enter the debug context. To show a list of commands available from within the debug context, type help or ?.

General Debug Commands

The following section describes general debug commands can be executed from within the debug context.

help

Shows available commands.

list-all

List all available commands.

history

Shows a list of previously run commands.

quit

Exits the debug context.

fw_upgrade

To upgrade the controller's firmware, use the following command:

```
fw_upgrade <protocol>://<server ip|server name>/<path/image
name> [-f]
fw_upgrade OPTIONS
```

Syntax Description

`fw_upgrade`	Upgrade the controller's firmware
`<protocol>`	Protocol for image transfer (FTP, TFTP, HTTP, KERMIT)
`<OPTIONS>`	-p: protocol -s: server IP address or name -n: image name with path on the server -f: non-verbose mode -h: fw_upgrade help message

Defaults

None.

Example

```
ruckus# debug
ruckus(debug)# fw_upgrade ftp://<user>:<password>@<server ip>/
<image file>
```

delete-station

To deauthorize the station with the specified MAC address, use the following command.

```
delete-station <MAC>
```

Syntax Description

`delete-station`	Delete the station with the specified MAC address
`<MAC>`	The MAC address of the station that will be deleted

Defaults

None.

Example

```
ruckus# debug
ruckus(debug)# delete-station 00:10:77:01:00:01
The command was executed successfully.
```

restart-ap

To restart the device with the specified MAC address, use the `restart ap` command.

```
restart-ap <MAC>
```

Syntax Description

`restart-ap`	Restart the device with the specified MAC address
`<MAC>`	The MAC address of the device to be restarted

Defaults

None.

Example

```
ruckus# debug
ruckus(debug)# restart-ap 00:13:92:EA:43:01
The command was executed successfully.
```

load-custom-ap

To load an AP customization file, use the following command:

```
load-custom-ap <WORD>
```

wlaninfo

Configures and enables debugging of WLAN service settings.

```
wlaninfo <OPTIONS>
```

Syntax Description

wlaninfo	Enable logging of WLAN info
<OPTIONS>	Configure WLAN debug information options

Defaults

None.

Example

```
ruckus(debug)# wlaninfo -W
WLAN svc "ruckus1" (id=1):
  WLAN ID = 0, ref_cnt = 5
  SSID = "ruckus1" enabled
  Apply to 11a and 11g/b radios
  Closed system = No, Privacy = Enabled, ACL enabled Guest-WLAN = No
  WISPr-WLAN = No
  Access Policy = 0/0, Web Auth = No, grace period = 0 (0 means
disable), max clients = 100
  WMM = enabled priority = 0 uplink = DISABLE downlink = DISABLE
  Cipher = Clear Text Local bridging = Enabled, vlan = 1, dvlan =
Disabled, bgscan = Enabled
  wep key index = 0, wep key len = 0
  PAP message authenticator = Enabled, EAP-Failure = Disabled
  Num of VAP deployed: 4
    VAP: c4:10:8a:1f:d1:fc, number of stations = 1
    VAP: c4:10:8a:1f:d1:f8, number of stations = 0
    VAP: 04:4f:aa:0c:b1:0c, number of stations = 0
    VAP: 04:4f:aa:0c:b1:08, number of stations = 0
  ACL 1 (System): default=Allowed system-wide=yes
  Auth Policy:
    Auth Algorithms:RSN/PSK  RSN/Dynamic PSK
    Auth Server Type: None
    WPA Verson: WPA2
    WPA Auth and Key Managment: WPA PSK
    GTK life time = 28800 seconds, GTK Life size = 2000 Kpkts
```

```
    GMK life time = 86400 seconds, Strict Rekey = No
    WPA Group Cipher Suites:0x00000010
      CCMP
    WPA Pairwise Cipher Suites:0x00000010
      CCMP
  NASID Type:  = wlan-bssid
  PMK Cache Time:  = 43200
  PMK Cache for Reconnect:  = enabled
  Roaming Acct-Inerim-Update:  = disabled
  Called-Station-Id-type: 0
  Classification: enabled
  UDP Heuristic Classification: enabled
  Directed Multicast: enabled
  IGMP Snooping: enabled
  MLD Snooping: enabled
  ToS Classification: enabled
  Dot1p Classification: disabled
  Multicast Filter: disabled
  Directed Threshold: 5
  Priority: Voice:0   Video:2   Data:4   Background:6

*** Total WLAN Entries: 1 ***
wlaninfo -W
ruckus(debug)#
```

save_debug_info

Saves debug information.

```
save_debug_info <IP-ADDR> <FILE-NAME>
```

Syntax Description

`save_debug_info`	Save debug log file
`<IP-ADDR>`	The destination IP address
`<FILE-NAME>`	The destination file name

Defaults

None.

Example

```
ruckus(debug)# save_debug_info 192.168.11.26 log.log
Creating debug info file ...
Done
Sending debug info file to "log.log@192.168.11.26" ...
...
```

```
ruckus(debug)#
```

save-config

Upload the configuration file to the designated TFTP site.

```
save-config <IP-ADDR> <FILE-NAME>
```

Syntax Description

`save-config`	Upload the configuration file
`<IP-ADDR>`	The destination IP address
`<FILE-NAME>`	The destination file name

Defaults

None.

Example

```
ruckus(debug)# save-config 192.168.11.26 config.log
Creating backup config file
Done
Uploading backup config file
...
ruckus(debug)#
```

Show Commands

This section describes the show commands available within the debug context.

show ap

Displays a list of all approved devices.

```
show ap
```

Syntax Description

`show ap`	Display a list of all approved APs

Defaults

None.

Example

```
ruckus(debug)# show ap
AP:
  ID:
    1:
      MAC Address= 04:4f:aa:0d:b1:00
```

```
      Model= zf7962
      Approved= Yes
      Device Name= 7962-MAP
      ...
      ...
ruckus(debug)#
```

show station

Displays a list of all connected stations (or clients).

```
show station
```

Syntax Description

`show station`	Show all connected stations

Defaults

None.

Example

```
ruckus(debug)# show station
Clients List:
  Client:
    MAC Address= 6c:62:6d:1b:e3:00
    User Name=
    IP Address= 192.168.11.11
    IPv6 Address=
    Access Point= 04:4f:aa:0c:b1:00
    WLAN= Ruckus1
    Channel= 1
    Signal (dB)= 53

  Client:
    MAC Address= 00:22:fb:ad:1b:2e
    User Name=
    IP Address= 192.168.11.7
    IPv6 Address=
    Access Point= 04:4f:aa:0c:b1:00
    WLAN= Ruckus1
    Channel= 165
    Signal (dB)= 42

ruckus(debug)#
```

show logs

Displays a list of debug log components.

```
show logs
```

Syntax Description

`show logs`	Display debug log components

Defaults

None.

Example

```
ruckus(debug)# show logs
Debug Logs:
  All= Enabled
  Sys-mgmt= Enabled
  Mesh= Enabled
  Web-auth= Enabled
  Rf-mgmt= Enabled
  Radius= Enabled
  Hotspot-srv= Enabled
  Aps= Enabled
  Net-mgmt= Enabled
  802.1x= Enabled
  Web-svr= Enabled
  802.11= Enabled
  Dvlan= Enabled
  Smart-redundancy= Enabled
  Debug logs of specified MAC address:
    Status= Disabled
ruckus(debug)#
```

show remote-troubleshooting

Shows remote-troubleshooting status.

```
show remote-troubleshooting
```

Syntax Description

`show remote-troubleshooting`	Display remote troubleshooting status

Defaults

None.

Example

ruckus(debug)# **show remote-troubleshooting**

Ruckus CA troubleshooting is stopped!

The server addr is: None

ruckus(debug)#

ps

Displays information about all processes that are running (ps -aux).

```
ps
```

Syntax Description

ps	Display a list of all running processes

Defaults

None.

Example

```
ruckus(debug)# ps
  PID PPID USER       VSZ STAT COMMAND
    1     0 ruckus    1200 S    init
    2     1 ruckus       0 SWN  [ksoftirqd/0]
    3     1 ruckus       0 SW   [watchdog/0]
    4     1 ruckus       0 SW<  [events/0]
    5     1 ruckus       0 SW<  [khelper]
    6     1 ruckus       0 SW<  [kthread]
    7     6 ruckus       0 SW<  [kblockd/0]
    8     6 ruckus       0 SW<  [khubd]
    9     6 ruckus       0 SW   [pdflush]
   10     6 ruckus       0 SW   [pdflush]
   12     6 ruckus       0 SW<  [aio/0]
   11     1 ruckus       0 SW   [kswapd0]
   13     1 ruckus       0 SW   [mtdblockd]
   14     6 ruckus       0 SW<  [scsi_eh_0]
   15     6 ruckus       0 SW<  [usb-storage]
   17     6 ruckus       0 SW<  [V54_bodygard/0]
   18     1 ruckus       0 SW   [pktgen/0]
   29     6 ruckus       0 SW<  [reiserfs/0]
  104     1 ruckus     956 S    /usr/sbin/in.tftpd -l -s /etc/
airespider-images
  110     1 ruckus     660 S    /bin/wd_feeder
  242     1 ruckus    2572 S    /bin/emf_repo_flashsync monitor 15
  243     1 ruckus     944 S    ttylogd
  246     1 ruckus       0 SW<  [uif-246]
  260     1 ruckus   14492 S    stamgr -d3 -t0
  266   260 ruckus   14492 S    stamgr -d3 -t0
  267   266 ruckus   14492 S <  stamgr -d3 -t0
  268   266 ruckus   14492 S    stamgr -d3 -t0
```

```
  269     1 ruckus    2268 S    apmgr
  277   269 ruckus    2268 S    apmgr
  278   277 ruckus    2268 S <  apmgr
  299     1 ruckus   19564 S    emfd
  316   299 ruckus   19564 S    emfd
  317   316 ruckus   19564 S    emfd
  318   316 ruckus   19564 S    emfd
  322     1 ruckus    1108 S    /usr/sbin/dropbear -e /bin/login.sh
-r /etc/air
  328     1 ruckus    1188 S    /bin/sh /bin/login.sh
  329     1 ruckus    1188 S    /bin/sh /bin/tacmon.sh
  331     1 ruckus     676 S    /bin/rhttpd
  332     1 ruckus    1140 S <  /bin/zapd
  333     1 ruckus    1100 S <  /bin/clusterD
  334   328 ruckus     856 S    /bin/login
  335   329 ruckus     680 S    /bin/tacmon -i 30 -r 15
  347     1 ruckus     808 S    /bin/tsyslogd -r -h -n --rotate=7
  368   277 ruckus    2268 S <  apmgr
  369   277 ruckus    2268 S <  apmgr
  572     1 ruckus    1184 S    /sbin/udhcpp -i br0 --pidfile=/var/
run/udhcpp.p
  580   316 ruckus   19564 S    emfd
  612   316 ruckus   19564 S    emfd
  616   316 ruckus   19564 S    emfd
  622   316 ruckus   19564 S    emfd
  624   299 ruckus    6132 S <  webs &
  625   316 ruckus   19564 S    emfd
  637   624 ruckus    6132 S    webs &
  638   637 ruckus    6132 S <  webs &
  639   637 ruckus    6132 S <  webs &
  640   637 ruckus    6132 S <  webs &
  641   637 ruckus    6132 S <  webs &
  642   637 ruckus    6132 S    webs &
  655   637 ruckus    6132 S <  webs &
  656   637 ruckus    6132 S <  webs &
20503   316 ruckus   19564 S    emfd
30679     1 ruckus    2672 S    /usr/sbin/vsftpd /etc/vsftpd2.conf
10220   322 ruckus    1184 S    /usr/sbin/dropbear -e /bin/login.sh
-r /etc/air
10221 10220 ruckus    1188 S    /bin/sh /bin/login.sh
10222 10221 ruckus     856 S    /bin/login
10223 10222 ruckus    7972 S    ruckus_cli2
10426 10223 ruckus    1188 S    sh -c /bin/ps -aux
```

```
10427 10426 ruckus    1188 R    /bin/ps -aux
ruckus(debug)#
```

Accessing a Remote AP CLI

The following command is used to access the command line interface of a connected AP and execute AP CLI commands from ZoneDirector. Configuration changes made through the AP CLI may be overwritten by ZoneDirector settings if the AP is restarted or reconnects to ZoneDirector.

remote_ap_cli

Use the remote_ap_cli command to access an AP remotely and execute AP CLI commands.

```
remote_ap_cli [-q] {-a ap_mac | -A } "cmd arg1 arg2 .."
```

Syntax Description

`remote_ap_cli`	Execute CLI commands in a remote AP
`-q`	Do not display results
`-a`	Specify AP by MAC address
`ap_mac`	The AP's MAC address
`-A`	All connected APs
`cmd`	AP CLI command
`arg`	AP CLI command argument

Defaults

None.

Example

```
rruckus(debug)# remote_ap_cli -A get director
---- Command 'rkscli -c "get director "' executed at
04:4f:aa:0c:b1:00
------ ZoneDirector Info ------
Primary Controller   : n/a
Secondary Controller : n/a
DHCP Opt43 Code      : 3

The information of the most recent Zone Director:
  [1] 192.168.11.100

  AP is under management of ZoneDirector: 192.168.11.100 / :: /
00:13:11:01:01:01,
  Currently AP is in state: RUN
```

```
OK
---- Command 'rkscli -c "get director "' executed at
c4:10:8a:1f:d1:f0
------ ZoneDirector Info ------
Primary Controller   : n/a
Secondary Controller : n/a
DHCP Opt43 Code      : 3

The information of the most recent Zone Director:
  [1] 192.168.11.100

  AP is under management of ZoneDirector: 192.168.11.100 / :: /
00:13:11:01:01:01,
  Currently AP is in state: RUN
OK
---- Command Execution Summary:
         success: 2
         failure: 0
           total: 2
rksap_cli -A get director
ruckus(debug)#
```

Working with Debug Logs and Log Settings

This section describes the commands that you can use to configure and review ZoneDirector debug logs.

logs all

Enables debug logs of all debug components.

Syntax Description

`logs all`	Enable logging of all debug components

Defaults

None.

Example

```
ruckus(debug)# logs all
The command was executed successfully.
ruckus(debug)# show logs
Debug Logs:
  All= Enabled
  Sys-mgmt= Enabled
```

```
  Mesh= Enabled
  Web-auth= Enabled
  Rf-mgmt= Enabled
  Radius= Enabled
  Hotspot-srv= Enabled
  Aps= Enabled
  Net-mgmt= Enabled
  802.1x= Enabled
  Web-svr= Enabled
  802.11= Enabled
  Dvlan= Enabled
  Smart-redundancy= Enabled
  Debug logs of specified MAC address:
    Status= Disabled
ruckus(debug)#
```

logs comp sys-mgmt

Enables debug logs of system management components.

Syntax Description

`logs`	Enable debug logs
`comp sys-mgmt`	Component system management

Defaults

None.

Example

```
ruckus(debug)# logs comp sys-mgmt
The command was executed successfully.
ruckus(debug)# show logs
Debug Logs:
  All= Disabled
  Sys-mgmt= Enabled
  Mesh= Disabled
  Web-auth= Disabled
  Rf-mgmt= Disabled
  Radius= Disabled
  Hotspot-srv= Disabled
  Aps= Disabled
  Net-mgmt= Disabled
  802.1x= Disabled
  Web-svr= Disabled
```

```
  802.11= Disabled
  Dvlan= Disabled
  Smart-redundancy= Disabled
  Debug logs of specified MAC address:
    Status= Disabled
ruckus(debug)#
```

logs comp mesh

Enables debug logs of mesh components.

Syntax Description

`logs`	Enable debug logs
`comp mesh`	Component mesh

Defaults

None.

Example

```
ruckus(debug)# logs comp mesh
The command was executed successfully.
ruckus(debug)#
```

logs comp web-auth

Enables debug logs of web authentication components.

Syntax Description

`logs`	Enable debug logs
`comp web-auth`	Component web auth

Defaults

None.

Example

```
ruckus(debug)# logs comp web-auth
The command was executed successfully.
ruckus(debug)#
```

logs comp rf-mgmt

Enables debug logs of RF management components.

Syntax Description

`logs`	Enable debug logs
`comp rf-mgmt`	Component RF management

Defaults

None.

Example

```
ruckus(debug)# logs comp rf-mgmt
The command was executed successfully.
ruckus(debug)#
```

logs comp radius

Enables debug logs of radius components.

Syntax Description

`logs`	Enable debug logs
`comp radius`	Component RADIUS

Defaults

None.

Example

```
ruckus(debug)# logs comp radius
The command was executed successfully.
ruckus(debug)#
```

logs comp hotspot-srv

Enables debug logs of hotspot services components.

Syntax Description

`logs`	Enable debug logs
`comp hotspot-srv`	Component Hotspot services

Defaults

None.

Example

```
ruckus(debug)# logs comp hotspot-srv
The command was executed successfully.
ruckus(debug)#
```

logs comp aps

Enables debug logs of AP components.

Syntax Description

`logs`	Enable debug logs
`comp aps`	Component APs

Defaults None.

Example

```
ruckus(debug)# logs comp aps
The command was executed successfully.
ruckus(debug)#
```

logs comp net-mgmt

Enables debug logs of network management components.

Syntax Description

`logs`	Enable debug logs
`comp net-mgmt`	Component network management

Defaults None.

Example

```
ruckus(debug)# logs comp net-mgmt
The command was executed successfully.
ruckus(debug)#
```

logs comp 802.1x

Enables debug logs of 802.1x components.

Syntax Description

`logs`	Enable debug logs
`comp 802.1x`	Component 802.1x

Defaults None.

Example

```
ruckus(debug)# logs comp 802.1x
```

```
The command was executed successfully.
ruckus(debug)#
```

logs comp web-svr

Enables debug logs of web server components.

Syntax Description

`logs`	Enable debug logs
`comp web-svr`	Component Web server

Defaults

None.

Example

```
ruckus(debug)# logs comp web-svr
The command was executed successfully.
ruckus(debug)#
```

logs comp 802.11

Enables debug logs of 802.11 components.

Syntax Description

`logs`	Enable debug logs
`comp 802.11`	Component 802.11

Defaults

None.

Example

```
ruckus(debug)# logs comp 802.11
The command was executed successfully.
ruckus(debug)#
```

logs comp dvlan

Enables debug logs of dynamic VLAN components.

Syntax Description

`logs`	Enable debug logs
`comp dvlan`	Component dynamic VLAN

Defaults None.

Example

```
ruckus(debug)# logs comp dvlan
The command was executed successfully.
ruckus(debug)#
```

logs comp smart-redundancy

Enables debug logs of smart redundancy components.

Syntax Description

`logs`	Enable debug logs
`comp smart-redundancy`	Component Smart Redundancy

Defaults None.

Example

```
ruckus(debug)# logs comp smart-redundancy
The command was executed successfully.
ruckus(debug)#
```

logs mac

Enables and sets filter running logs based on specified mac address.

```
logs mac <MAC>
```

Syntax Description

`logs`	Enable debug logs
`mac`	Filter logs by specific MAC address
`<MAC>`	The MAC address of the device to be filtered

Defaults None.

Example

```
ruckus(debug)# logs mac 04:4f:aa:0c:b1:00
The command was executed successfully.
ruckus(debug)#
```

logs play

Starts displaying logs on console.

Syntax Description

`logs`	Enable debug logs
`play`	Start log play

Defaults

None.

Example

```
ruckus(debug)# logs play
ruckus(debug)# [Feb 15 05:53:30][EMFD][debug]jobService-
Func():Executing job[user auth attempt_hash_autoexpire] at
1329285210...
[Feb 15 05:53:30][EMFD][debug]jobServiceFunc():Executing job at
1329285210...Done
[Feb 15 05:53:30][EMFD][debug]jobServiceFunc():Executing
job[station auth attempt_hash_autoexpire] at 1329285210...
[Feb 15 05:53:30][EMFD][debug]jobServiceFunc():Executing job at
1329285210...Done
[Feb 15 05:53:33][STAMgr][debug]acsrvc_thread():ACSRVC rcv AP
04:4f:aa:0c:b1:00, IP= 192.168.11.6, IPv6=fc00::1
...
...
ruckus(debug)# no logs play
ruckus(debug)#
```

no logs all

Disables debug logs of all debug components.

Syntax Description

`no logs`	Disable debug logs
`all`	Disable all log components

Defaults

None.

Example

```
ruckus(debug)# no logs all
The command was executed successfully.
ruckus(debug)#
```

no logs comp sys-mgmt

Disables debug logs of system management components.

Syntax Description

`no logs`	Disable debug logs
`comp sys-mgmt`	Component system management

Defaults

None.

Example

```
ruckus(debug)# no logs comp sys-mgmt
The command was executed successfully.
ruckus(debug)#
```

no logs comp mesh

Disables debug logs of mesh components.

Syntax Description

`no logs`	Disable debug logs
`comp mesh`	Component Mesh

Defaults

None.

Example

```
ruckus(debug)# no logs comp mesh
The command was executed successfully.
ruckus(debug)#
```

no logs comp web-auth

Disables debug logs of web authentication components.

Syntax Description

`no logs`	Disable debug logs
`comp web-auth`	Component Web authentication

Defaults

None.

Example

```
ruckus(debug)# no logs comp web-auth
```

```
The command was executed successfully.
ruckus(debug)#
```

no logs comp rf-mgmt

Disables debug logs of RF management components.

Syntax Description

`no logs`	Disable debug logs
`comp rf-mgmt`	Component RF management

Defaults

None.

Example

```
ruckus(debug)# no logs comp rf-mgmt
The command was executed successfully.
ruckus(debug)#
```

no logs comp radius

Disables debug logs of radius components.

Syntax Description

`no logs`	Disable debug logs
`comp radius`	Component RADIUS

Defaults

None.

Example

```
ruckus(debug)# no logs comp radius
The command was executed successfully.
ruckus(debug)#
```

no logs comp hotspot-srv

Disables debug logs of hotspot services components.

Syntax Description

`no logs`	Disable debug logs
`comp hotspot-srv`	Component Hotspot services

Defaults

None.

Example

```
ruckus(debug)# no logs comp hotspot-srv
The command was executed successfully.
ruckus(debug)#
```

no logs comp aps

Disables debug logs of access points components.

Syntax Description

`no logs`	Disable debug logs
`comp aps`	Component APs

Defaults

None.

Example

```
ruckus(debug)# no logs comp aps
The command was executed successfully.
ruckus(debug)#
```

no logs comp net-mgmt

Disables debug logs of network management components.

Syntax Description

`no logs`	Disable debug logs
`comp net-mgmt`	Component network management

Defaults

None.

Example

```
ruckus(debug)# no logs comp net-mgmt
The command was executed successfully.
ruckus(debug)#
```

no logs comp 802.1x

Disables debug logs of 802.1x components.

Syntax Description

`no logs`	Disable debug logs
`comp 802.1x`	Component 802.1x

Defaults

None.

Example

```
ruckus(debug)# no logs comp 802.1x
The command was executed successfully.
ruckus(debug)#
```

no logs comp web-svr

Disables debug logs of web server components.

Syntax Description

`no logs`	Disable debug logs
`comp web-svr`	Component Web server

Defaults

None.

Example

```
ruckus(debug)# no logs comp web-svr
The command was executed successfully.
ruckus(debug)#
```

no logs comp 802.11

Disables debug logs of 802.11 components.

Syntax Description

`no logs`	Disable debug logs
`comp 802.11`	Component 802.11

Defaults

None.

Example

```
ruckus(debug)# no logs comp 802.11
The command was executed successfully.
ruckus(debug)#
```

no logs comp dvlan

Disables debug logs of dynamic vlan components.

Syntax Description

`no logs`	Disable debug logs
`comp dvlan`	Component DVLAN

Defaults

None.

Example

```
ruckus(debug)# no logs comp dvlan
The command was executed successfully.
ruckus(debug)#
```

no logs comp smart-redundancy

Disables debug logs of smart redundancy components.

Syntax Description

`no logs`	Disable debug logs
`comp smart-redundancy`	Component Smart Redundancy

Defaults

None.

Example

```
ruckus(debug)# no logs comp smart-redundancy
The command was executed successfully.
ruckus(debug)#
```

no logs mac

Disables MAC address filtering on running logs.

Syntax Description

`no logs`	Disable debug logs
`mac`	Filter by MAC address

Defaults

None.

Example

```
ruckus(debug)# no logs mac
The command was executed successfully.
ruckus(debug)#
```

no logs play

Stops displaying logs on console.

Syntax Description

`no logs`	Disable debug logs
`play`	Stop log play

Defaults

None.

Example

```
rruckus(debug)# logs play
ruckus(debug)# [Feb 15 05:53:30][EMFD][debug]jobService-
Func():Executing job[user auth attempt_hash_autoexpire] at
1329285210...
[Feb 15 05:53:30][EMFD][debug]jobServiceFunc():Executing job at
1329285210...Done
[Feb 15 05:53:30][EMFD][debug]jobServiceFunc():Executing
job[station auth attempt_hash_autoexpire] at 1329285210...
[Feb 15 05:53:30][EMFD][debug]jobServiceFunc():Executing job at
1329285210...Done
[Feb 15 05:53:33][STAMgr][debug]acsrvc_thread():ACSRVC rcv AP
04:4f:aa:0c:b1:00, IP= 192.168.11.6, IPv6=fc00::1
...
...
ruckus(debug)# no logs play
ruckus(debug)#
```

Remote Troubleshooting

This section describes remote troubleshooting commands.

remote-troubleshooting server

To set the remote troubleshooting server IP address, use the following command:

```
remote-troubleshooting server <IP-ADDR>
```

remote-troubleshooting start

Enables remote troubleshooting.

Syntax Description

`remote-troubleshooting`	Remote troubleshooting
`start`	Start remote troubleshooting

Defaults

None.

Example

```
ruckus(debug)# remote-troubleshooting start


ruckus(debug)#
```

remote-troubleshooting stop

Disables remote troubleshooting.

Syntax Description

`remote-troubleshooting`	Remote troubleshooting
`stop`	Stop remote troubleshooting

Defaults

None.

Example

```
ruckus(debug)# remote-troubleshooting stop

ruckus(debug)#
```

AP Core Dump Collection

This section lists the AP core dump commands.

collect_ap_coredump

Enable AP core dump collection.

```
collect_ap_coredump [all|<MAC>]
```

Syntax Description

`collect_ap_coredump`	Collect AP core dump
`all`	Collect core dump from all connected APs
`<MAC>`	Specific AP MAC address

Defaults

None.

Example

```
ruckus(debug)# collect_ap_coredump all
---- Command 'apmgrinfo --coredump y ' executed at 04:4f:aa:0c:b1:00
start reporting coredump to ZD!
---- Command 'apmgrinfo --coredump y ' executed at 00:24:82:3f:14:60
start reporting coredump to ZD!
---- Command Execution Summary:
         success: 2
         failure: 0
```

```
           total: 2
rm: cannot remove '/etc/airespider-images/firmwares/ap-dump/*': No
such file or directory
sh: codump_server: not found
start collecting AP's coredump !
ok
ruckus(debug)#
```

no collect_ap_coredump

Disable AP core dump collection.

Syntax Description

`no collect_ap_coredump`	Stop collecting AP core dump

Defaults

None.

Example

```
ruckus(debug)# no collect_ap_coredump all
---- Command 'apmgrinfo --coredump n ' executed at 04:4f:aa:0c:b1:00
stop reporting coredump to ZD!
---- Command 'apmgrinfo --coredump n ' executed at 00:24:82:3f:14:60
stop reporting coredump to ZD!
---- Command Execution Summary:
         success: 2
         failure: 0
           total: 2
rm: cannot remove '/etc/airespider-images/firmwares/ap-dump/*': No
such file or directory
stop collecting AP's coredump !
ok
ruckus(debug)#
```

Script Execution

This section lists the commands that can be executed from the script context. The script context must be entered from the debug context.

script

Enters the script context from the debug context. You must first enter the script context before executing a script.

```
script
```

Syntax Description

`script`	Enter the script context

Defaults

None.

Example

```
ruckus(debug)# script
ruckus(script)#
```

quit

Exit the script context.

```
quit
```

Syntax Description

`quit`	Exit the script context

Defaults

None.

Example

```
ruckus(script)# quit
ruckus(debug)#
```

list

List all available scripts.

```
list
```

Syntax Description

`list`	List all available scripts

Defaults

None.

Example

```
ruckus(script)# list -a

 Index                          Scripts
     1                       .version.sh
```

```
ruckus(script)#
```

del

Deletes a script.

info

Display script help file

```
info
```

Syntax Description

`info`	Display script information

Defaults

None.

Example

```
ruckus(script)# info
info <file>
ruckus(script)#
```

exec

Execute script.

```
exec <file> {parameter}
```

Syntax Description

`exec`	Excecute the script

Defaults

None.

Example

```
ruckus(script)# exec
exec <file> {parameter}
ruckus(script)#
```

Index

Numerics

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z