RUCKUS
COMMSCOPE

RUCKUS Unleashed 200.16 Command Line Interface Reference Guide

Supporting Unleashed 200.16

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

Limitation of Liability

Trademarks

CommScope and the CommScope logo are registered trademarks of CommScope and/or its affiliates in the U.S. and other countries. For additional trademark information see https://www.commscope.com/trademarks. All product names, trademarks, and registered trademarks are the property of their respective owners.

Patent Marking Notice

For applicable patents, see www.cs-pat.com.

Contents

Contact Information, Resources, and Conventions

Contacting RUCKUS Customer Services and Support

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their RUCKUS products, and to customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the RUCKUS Support Portal using https://support.ruckuswireless.com, or go to https://www.ruckusnetworks.com and select **Support**.

What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources, use the following criteria:

* Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Submit a Case** section.
* Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Submit a Case** section.
* Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Click the **CONTACT** tab at the top of the page and explore the **Self-Service Online Help** options.
* Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Click the **CONTACT** tab at the top of the page and explore the **Self-Service Online Help** options.

Open a Case

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

* Continental United States: 1-855-782-5871
* Canada: 1-855-782-5871
* Europe, Middle East, Africa, Central and South America, and Asia Pacific, toll-free numbers are available at https://support.ruckuswireless.com/contact-us and Live Chat is also available.
* Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

We suggest that you keep a physical note of the appropriate support number in case you have an entire network outage.

Self-Service Resources

The RUCKUS Support Portal at https://support.ruckuswireless.com offers a number of tools to help you to research and resolve problems with your RUCKUS products, including:

- Technical Documentation—https://support.ruckuswireless.com/documents

- Community Forums—https://community.ruckuswireless.com

- Knowledge Base Articles—https://support.ruckuswireless.com/answers

- Software Downloads and Release Notes—https://support.ruckuswireless.com/#products_grid

- Security Bulletins—https://support.ruckuswireless.com/security

Using these resources will help you to resolve some issues, and will provide the Technical Assistance Center (TAC) with additional data from your troubleshooting analysis if you still require assistance through a support case or Return Merchandise Authorization (RMA). If you still require help, open and manage your case at https://support.ruckuswireless.com/case_management.

Document Feedback

RUCKUS is interested in improving its documentation and welcomes your comments and suggestions.

You can email your comments to RUCKUS at #Ruckus-Docs@commscope.com.

When contacting us, include the following information:

- Document title and release number

- Document part number (on the cover page)

- Page number (if appropriate)

For example:

- RUCKUS SmartZone Upgrade Guide, Release 5.0

- Part number: 800-71850-001 Rev A

- Page 7

RUCKUS Product Documentation Resources

Visit the RUCKUS website to locate related documentation for your product and additional RUCKUS resources.

Release Notes and other user documentation are available at https://support.ruckuswireless.com/documents. You can locate the documentation by product or perform a text search. Access to Release Notes requires an active support contract and a RUCKUS Support Portal user account. Other technical documentation content is available without logging in to the RUCKUS Support Portal.

White papers, data sheets, and other product documentation are available at https://www.ruckusnetworks.com.

Online Training Resources

To access a variety of online RUCKUS training modules, including free introductory courses to wireless networking essentials, site surveys, and products, visit the RUCKUS Training Portal at https://commscopeuniversity.myabsorb.com/. The registration is a two-step process described in this video. Create a CommScope account and then register for, and request access for, CommScope University.

Document Conventions

The following table lists the text conventions that are used throughout this guide.

TABLE 1 Text Conventions

Convention	Description	Example
monospace	Identifies command syntax examples	`device(config)# interface ethernet 1/1/6`
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	Publication titles	Refer to the *RUCKUS Small Cell Release Notes* for more information.

Notes, Cautions, and Safety Warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

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

ATTENTION
An ATTENTION statement indicates some information that you must read before continuing with the current action or task.

CAUTION
A CAUTION statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER
A DANGER statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Command Syntax Conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional.
	Default responses to system prompts are enclosed in square brackets.
{**x**| **y**| **z**}	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x|**y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

About This Guide

Introduction

The *RUCKUS Unleashed CLI Reference Guide* contains the syntax and commands for configuring and managing Unleashed from a command line interface.

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

> **NOTE**
> If release notes are shipped with your product and the information there differs from the information in this guide, follow the instructions in the release notes.

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

https://support.ruckuswireless.com/documents.

New in This Release

The following sections list the changes in CLI commands for Unleashed 200.16.

New Commands for Unleashed 200.16

The following commands have been added (new for this release).

- **qos-mirroring**
- **transition-disable**

Modified Commands for Unleashed 200.16

The following commands have been modified (updated for this release).

- **radio**
- **show performance**
- **background-scan**
- **wlan-bind**
- **bss-priority**
- **wifi6/7**

Deprecated Commands for Unleashed 200.16

The following commands have been deprecated in this release.

- **usb-software**
- **show usb-software**
- **usb-port**
- **usb-port-overide**
- **url-filtering-expire-timeout**
- **url-filtering-license-server**

Understanding the Unleashed Command Line Interface

Introduction

The RUCKUS Unleashed Command Line Interface (CLI) is a software tool that allows you to configure and manage your Unleashed network - including the Unleashed Master AP and all currently managed member APs - using CLI commands.

Using the command line interface, you can configure Unleashed Master AP system settings, access points, wireless networks and client connection settings, or view current status information for each component of your RUCKUS Unleashed wireless network. 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 Unleashed CLI.

> **NOTE**
> The Unleashed CLI supports a maximum of 8 simultaneous SSH sessions, and a maximum 4 sessions from the same IP address.

Requirements

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

- A computer that you will designate as the admin computer
- A network connection to the Unleashed Master AP
- An SSH (secure shell) client such as PuTTY

Step 1: Connecting the Administrative Computer to Unleashed

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

- Using an Ethernet Connection on page 30
- Using a Serial Connection on page 30

Step 2: Start and Configure the SSH Client

Before starting this procedure, make sure that your 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 Unleashed 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*.

Using an Ethernet Connection

1. Ensure that Unleashed's IP address is reachable from the administrative computer. In factory default state, Unleashed's IP address is **192.168.0.1**.

2. Continue to *"Step 2: Start and Configure the SSH Client"*.

Using a Serial Connection

To start and configure the 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 1 Select Serial as the connection type
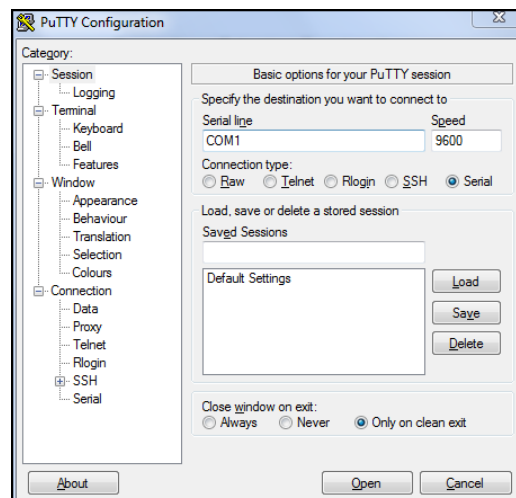
3. Under **Category**, click **Connection** > **Serial**. The serial connection options appear on the right side of the dialog box, displaying PuTTY's default serial connection settings.

    FIGURE 2 PuTTY's default serial connection settings
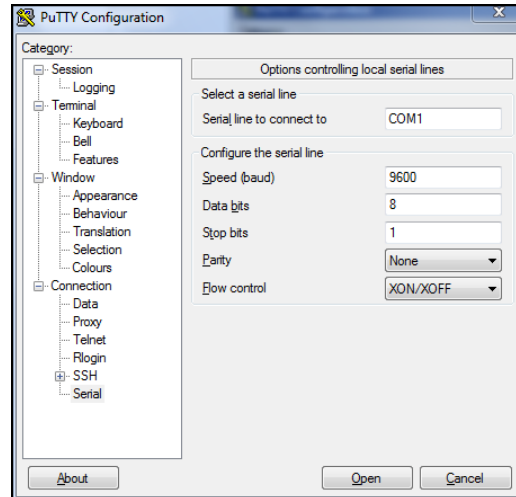
4. Configure the serial connection settings as follows:

    - **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 3 PuTTY's serial connection settings for connecting to Unleashed
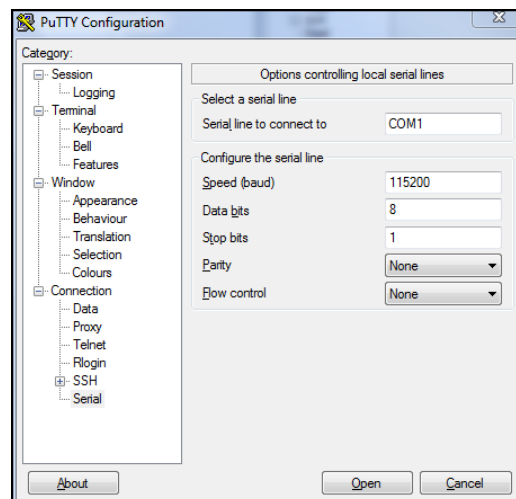
5. Click **Open**. The PuTTY console appears and displays the login prompt.

FIGURE 4 The PuTTY console displaying the login prompt
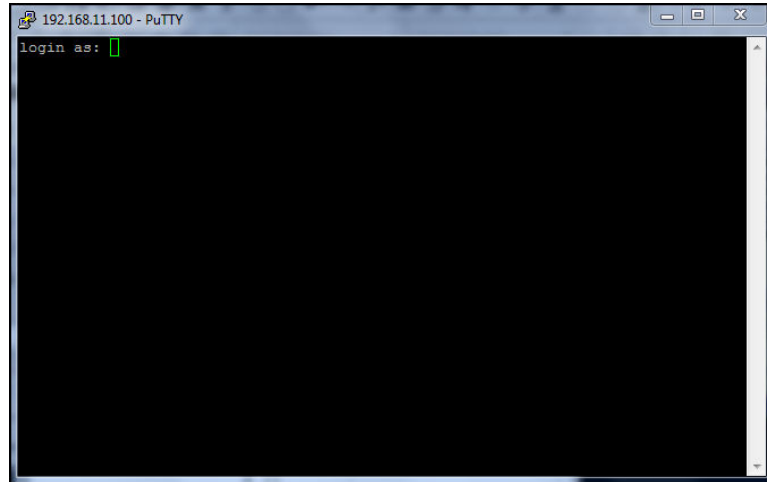
You have completed configuring the Telnet/SSH client to connect to Unleashed.

Step 3: Log Into the CLI

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

2. At the **Please login** prompt, enter the login name (default: **super**), and then press **<Enter>**.

3. At the **Password** prompt, enter the login password (default: **sp-admin**), and then press **<Enter>**. The Unleashed CLI welcome message and the `ruckus>` prompt appears.

You are now logged into the Unleashed 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).
> 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**).

Unleashed CLI Setup Wizard

The CLI setup wizard allows you to quickly configure your controller with basic settings using a short series of CLI commands.

To perform Unleashed setup using CLI commands, use the following procedure:

1. When the Unleashed AP is in factory default state, associate to the "Configure.Me-xxxxxx" WLAN and connect to the Unleashed CLI using SSH (default address: **10.154.231.125**), and log in using the default user name and password:

   - Please login: **super**

   - Password: **sp-admin**

   The Unleashed CLI Wizard Configuration tool starts automatically.

2. Follow the instructions in the setup wizard to configure your Unleashed Master AP. Following are the examples.

Configure Unleashed AP in Bridge Mode - Local Wizard

```
Would you like to start the Setup Wizard? [yes/no]: yes

Enter the way of installation:

1. easy-deployment installation.(Warning: The configuration costs about 15 seconds to store in system, and
in flash empase the device may be damaged if power-off. So please avoid rebooting device after 60 seconds
if network is reachable)

2. local wizard

please enter 1 or 2:
2

Enter Administrative User Name (32 characters max) [admin]:
admin
Enter Administrator Password (4-32 characters):
*****
Re-enter Administrator Password (4-32 characters):
*****

Enter System Name (32 characters max) [Ruckus-Unleashed]:
Unleashed

Enter Country Code (or 'help' to show the list) [US]: US

Enable Mesh [yes/NO]? no

Enable Gateway Mode [yes/NO]? no

Enable Dedicated Master [yes/NO]? no

Enter WAN IP type [1]:
     1: DHCP Mode;
     2: Manual Mode;
1

Enter Access VLAN [1]:

Enable WLANs [YES/no]? yes

Enter Wireless LAN (ESSID, 1-32 characters) [Ruckus-Wireless 1]:
Unleashed-SSID
Is it an Open WLAN [yes/NO]? no
Enter the WPA2 Passphrase (8-63 characters): ********
Re-enter the WPA2 Passphrase (8-63 characters):
********

Please review the following settings:
System Name=                  Ruckus-Unleashed
```

```
Administrator Name=          admin
Country Code=                US
Mesh Supported=              Disable
Gateway Mode Supported=      Disable
Dedicated Master Supported= Disable
IPv4 Mode=                   DHCP
Access VLAN=                 1
WLAN ESSID=                  Ruckus-Wireless 1
Wireless Authentication=     WPA2_PSK


Done with the Setup Wizard [yes/no]? yes

Save the configuration ...



It will take a few minutes to complete, do not power off the AP! This AP will reboot automatically.

Welcome to Ruckus Unleashed Network Command Line Interface
ruckus>
```

Configure Unleashed AP in Bridge Mode - Easy Deployment Installation

```
Would you like to start the Setup Wizard? [yes/no]: y

Enter the way of installation:

1. easy-deployment installation.(Warning: The configuration costs about 15 seconds to store in system, and
in flash empase the device may be damaged if power-off. So please avoid rebooting device after 60 seconds
if network is reachable)

2. local wizard

please enter 1 or 2:
1

Enter System Name (32 characters max) [Ruckus-Unleashed]:


System name is set as [Ruckus-Unleashed]


Enter the umm server ip or host (63 characters max):umm_server

Enter the tag (16 characters limited, only number, alphabet, underscores(_),period(.), hyphens(-), at(@)
characters are allowed ):

Easy-deployment is running now. It will take a few minutes

Welcome to Ruckus Unleashed Network Command Line Interface
```

Configure Unleashed AP in Dedicated Mode

```
Please login: super
Password: ********


Welcome to Ruckus Wireless Unleashed CLI Command Line Interface


Would you like to start the Setup Wizard? [yes/no]: yes

Enter the way of installation:

1. easy-deployment installation.(Warning: The configuration costs about 15 seconds to store in system, and
in flash empase the device may be damaged if power-off. So please avoid rebooting device after 60 seconds
if network is reachable)

2. local wizard
```

```
please enter 1 or 2:
2

Enter Administrative User Name (32 characters max) [admin]:
admin
Enter Administrator Password (4-32 characters):
*****
Re-enter Administrator Password (4-32 characters):
*****

Enter System Name (32 characters max) [Ruckus-Unleashed]:
Unleashed

Enter Country Code (or 'help' to show the list) [US]: US

Enable Mesh [yes/NO]? yes

Enable Gateway Mode [yes/NO]?

Enable Dedicated Master [yes/NO]? yes

Enter WAN IP type [1]:
     1: DHCP Mode;
     2: Manual Mode;
1
Enter Access VLAN [1]: 1

Enable WLANs [YES/no]?

Enter Wireless LAN (ESSID, 1-32 characters) [Ruckus-Wireless 1]:
Dedicated-SSID
Is it an Open WLAN [yes/NO]?
Enter the WPA2 Passphrase (8-63 characters):
********
Re-enter the WPA2 Passphrase (8-63 characters):
********

Please review the following settings:
System Name=              Unleashed
Administrator Name=       admin
Country Code=             US
Mesh Supported=           Enable
Gateway Mode Supported=   Disable
Dedicated Master Supported= Enable
    IPv4 Mode=            DHCP
    Access VLAN=          1
WLAN ESSID=               Dedicated-SSID
Wireless Authentication=  WPA2_PSK


Done with the Setup Wizard [yes/no]? yes


Save the configuration ...



It will take a few minutes to complete, do not power off the AP! This AP will reboot automatically.

Welcome to Ruckus Unleashed Network Command Line Interface
ruckus>
```

Configure Unleashed AP in Gateway Mode

```
Please login: super
Password: ********


Welcome to Ruckus Wireless Unleashed CLI Setup Wizard
```

```
Would you like to start the Setup Wizard? [yes/no]: yes

Enter Administrative User Name (32 characters max) [admin]:
admin
Enter Administrator Password (4-32 characters):
*****
Re-enter Administrator Password (4-32 characters):
*****

Enter System Name (32 characters max) [Ruckus-Unleashed]:
Unleashed-Gateway

Enter Country Code (or 'help' to show the list) [US]: US

Enable Mesh [yes/NO]? no

Enable Gateway Mode [yes/NO]? yes

Enter AP R720 WAN Port:
    1: port1, eth0, UP:
    2: port2, eth1, DOWN:
1

Enter WAN IP type [1]:
     1: DHCP Mode;
     2: Manual Mode;
     3: PPPOE Mode;
1

// if H350, H550 AP
Enable standby WAN port [yes/NO]? y
Enter AP H350 Standby WAN Port:
    1: port1, eth0, UP (Primary WAN):
    2: port2, eth1, UP:
2
Enter standby WAN IP type [1]:
     1: DHCP Mode;
     2: Manual Mode;
2
Enter IP Address: 10.223.55.88
Enter IP Mask:    255.255.255.0
Enter Gateway:    10.223.55.254
Enter Primary DNS Server:   10.10.10.190
Enter Secondary DNS Server: 10.10.10.105
Enter LAN & WLAN IP Address [10.106.0.1]:
192.168.1.1
Enter LAN & WLAN IP Netmask [255.255.0.0]:
255.255.255.0
Enter Client Starting IP Address [10.106.0.2]:
192.168.1.2
Enter Client Ending IP Address [10.106.7.209]:
192.168.1.200

Enter Lease Time [2]:
    1: 6 hours;
    2: 12 hours;
    3: 1 day;
    4: 2 days;
    5: 1 week;
    6: 2 weeks;

1

Enable WLANs [YES/no]? yes

Enter Wireless LAN (ESSID, 1-32 characters) [Ruckus-Wireless 1]:
Unleashed-SSID
Is it an Open WLAN [yes/NO]? no
Enter the WPA2 Passphrase (8-63 characters):
********
Re-enter the WPA2 Passphrase (8-63 characters):
********
```

```
Please review the following settings:
System Name=             Unleashed-Gateway
Administrator Name=      admin
Country Code=            US
Mesh Supported=          Disable
Gateway Mode Supported=  Enable
WAN Port=                port1 eth0 UP
IPv4 Mode=               DHCP
LAN Port IPv4 Address Info= 192.168.1.1/255.255.255.0
Client Starting IPv4=    192.168.1.2
Client Ending IPv4=      192.168.1.200
Lease Time=              6 hours
WLAN ESSID=              Unleashed-SSID
Wireless Authentication= WPA2_PSK


Done with the Setup Wizard [yes/no]? yes

Save the configuration ...



It will take a few minutes to complete, do not power off the AP! This AP will reboot automatically.

Welcome to Ruckus Unleashed Network Command Line Interface
ruckus>
```

Using the ? Command

To display a brief list of commands that are available within a specific context, use the **?** command.

Example

```
ruckus(config)# admin
ruckus(config-admin)# ?
  help                  Shows available commands.
  history               Shows a list of previously run commands.
  abort                 Exits the config-admin context without saving changes.
  end                   Saves changes, and then exits the config-admin context.
  exit                  Saves changes, and then exits the config-admin context.
  quit                  Exits the config-admin context without saving changes.
  name <WORD>           Sets the admin name.
  no                    Contains commands that can be executed from within the context.
  auth-server <WORD>    Enables administrator authentication with a remote server and sets the
                        authentication server to the specified address.
  show                  Displays administrative settings.
ruckus(config-admin)#
```

Using the Help Command

To display all commands that the RUCKUS CLI supports, use the **help** command.

NOTE

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* above for more information.

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 Master.
shutdown	Shut down Unleashed, to power on Unleashed again, press the power.
set-factory	Reset the Master to factory defaults.
data-privacy	Execute data privacy commands.
config	Enter the config context.
logo	Configure Ruckus logo. Options are "logo nodog" and "logo default."
easyDpl-get-status	Get easy-deployment running status.
easyDpl-disable	Debug command, please stop easy-deployment by Webpage. This command stops easy-deployment and disables tr069 function, may cause mechanism chaos when easy-deployment is after prepareimage status.
debug	Enter the debug context.
show	Display current system options and settings.
reset	Reset RADIUS statistics commands.
session-timeout <NUMBER>	Set the CLI session timeout.
ap-mode	Run AP CLI (set/get) in Master AP

disable

To disable privileged commands, use the following command:

disable

Example

```
ruckus# disable
ruckus>
```

ping

To send ICMP echo packets to an IP address or domain name, use the following command:

ping <IP-ADDR/DOMAIN-NAME>

Example

```
ruckus> ping google.com
PING google.com (172.217.6.142): 56 data bytes
64 bytes from 172.217.6.142: seq=0 ttl=56 time=40.252 ms
64 bytes from 172.217.6.142: seq=1 ttl=56 time=33.652 ms
```

```
64 bytes from 172.217.6.142: seq=2 ttl=56 time=32.560 ms

--- google.com ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 32.560/35.488/40.252 ms
ruckus>
```

reboot

To reboot the controller, use the following command:

reboot

Example

```
ruckus# reboot
ruckus#
```

shutdown

To shut down the controller, use the following command:

shutdown

Use this command to shut down ZoneDirector. To power on ZoneDirector again, press the power button. When the Status LED is lit steadily, you can then reconnect to the CLI.

Example

```
ruckus# shutdown
ruckus#
```

set-factory

To reset the controller to factory default settings, use the following command:

set-factory

Example

```
ruckus# set-factory
ruckus#
```

data-privacy

To execute data privacy PII (personally identifiable information) commands, use the following command:

data-privacy

Example

```
ruckus# data-privacy
You have all rights in this mode.
ruckus(data-privacy)#
  help                  Shows available commands.
```

```
    history            Shows a list of previously run commands.
    abort              Exits current context without saving changes.
    end                Saves changes, and then exits the current context.
    exit               Saves changes, and then exits the current context.
    quit               Exits current context without saving changes.
    show               Shows settings.
    search <MAC>       Search PII Data by device MAC.
    delete <MAC>       Delete PII Data by device MAC.
    ftpurl <FTP Url>   Enter the FTP URL like
                       ftp://[username:password@]serverip[:port][/subdirectory/]
ruckus(data-privacy)#
```

search

To Search PII Data by device MAC, use the following command:

search <MAC>

Example

```
    ruckus(data-privacy)# search 00:01:02:03:04:05
    Please input ftp url first
    ruckus(data-privacy)#
```

delete

To delete PII data by device MAC, use the following command:

delete <MAC>

Example

```
    ruckus(data-privacy)# delete 00:01:02:03:04:05
    Please input ftp url first
    ruckus(data-privacy)#
```

ftpurl

To configure the FTP URL for data privacy, use the following command:

ftpurl <FTP Url>

Enter the FTP URL in the following format:

ftp://[username:password@]serverip[:port][/subdirectory/]

Example

```
    ruckus(data-privacy)# ftpurl ftp://admin:admin@192.168.40.10:443/ftp
    FTP server is not reachable or wrong ftp url ftp://admin:admin@192.168.40.10:443/ftp
    ruckus(data-privacy)#
```

config

To enter the config context and configure the controller, use the following command:

config

Example

```
ruckus# config
You have all rights in this mode.
ruckus(config)#
```

logo

To enable or disable suppression of the RUCKUS dog logo, use the following command:

logo [nodog|default]

Example

```
ruckus# logo nodog
ln: /etc/airespider-images/oem/logo.png: File exists
ruckus# logo default
ln: /etc/airespider-images/oem/logo.png: File exists
ruckus#
```

debug

To enter the debug context to manage system debug options, use the following command:

debug

Example

```
ruckus# debug
You have all rights in this mode.
ruckus(debug)#
```

reset radius-statistics

To reset controller RADIUS statistics, use the following command:

reset radius-statistics [server-all|server-name <WORD>| wlan-all| wlan-name <NAME>

Example

```
ruckus# reset radius-statistics wlan-all
Reset all WLANs RADIUS statistics successfully
ruckus#
```

session-timeout

To configure the session timeout, use the following command:

Syntax

session-timeout <NUMBER>

Command Default

30 minutes

Examples

```
ruckus# session-timeout 30
The command was executed successfully.
ruckus#
```

ap-mode

To go to the local AP's CLI from the Master's CLI, use the following command:

Syntax

ap-mode

Examples

```
ruckus# ap-mode
You have all rights in this mode.
ruckus(ap-mode)#
```

easyDpl-get-status

Get easy-deployment running status.

Example

```
ruckus# easyDpl-get-status
The easy deployment status is: IDEL
ruckus#
```

easyDpl-disable

Debug command. This command stops easy-deployment and disables tr069 function.

NOTE

This command is for debugging use only. It may cause mechanism chaos when easy-deployment is enabled after prepare image is complete. The recommended way to disable this feature is through the web interface.

Viewing Current Configuration

Show Commands Overview

Show commands display the controller's current configuration and status information, 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

Displays information about the authentication, authorization, and accounting servers (AAA) servers that have been added to the controller.

show aaa [**all**|**name** *WORD*]

Parameters

all

> Displays information about all the AAA servers.

name

> Displays information about the specified AAA server name.

WORD

> Name of the AAA server.

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#

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 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 DHCP servers that have been configured on 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 DHCP servers that have been configured on 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= d4:c1:9e:35:c9:40
      Model= r610
      Approved= Yes
      Device Name= Ruckus-Unleashed
      Device Role= Master
      Description=
      Location=
      GPS=
      CERT = Normal
      Bonjour-policy=
      Bonjour-fencing=
      Group Name= System Default
      Channel Range:
        A/N= 36,40,44,48,149,153,157,161 (Disallowed= )
        B/G/N= 1,2,3,4,5,6,7,8,9,10,11 (Disallowed= )
      Radio a/n:
        Channelization= Auto
        Channel= Auto
        WLAN Services enabled= Yes
        Tx. Power= Auto
        WLAN Group Name= Default
        Call Admission Control= OFF
        Protection Mode= Auto
      Radio b/g/n:
        Channelization= Auto
        Channel= Auto
        WLAN Services enabled= Yes
        Tx. Power= Auto
```

```
          WLAN Group Name= Default
          Call Admission Control= OFF
          Protection Mode= 2
        Override global ap-model port configuration= No
        Network Setting:
          Protocol mode= IPv4-Only
          Device IP Settings= DHCP
          IP Address= 192.168.0.13
          Netmask= 255.255.255.0
          Gateway= 192.168.0.1
          Primary DNS Server= 66.90.130.101
          Secondary DNS Server= 216.82.201.11
        Mesh:
          Status= Disabled
        LLDP:
          Status = Use Parent Setting
        LAN Port:
          0:
            Interface= eth0
            Dot1x= None
            LogicalLink= Up
            PhysicalLink= Up 1000Mbps full
            Label= 10/100/1000 PoE Port1
          1:
            Interface= eth1
            Dot1x= None
            LogicalLink= Down
            PhysicalLink= Down
            Label= 10/100/1000 Port2
        PoE Mode= Auto
        802.3af PoE Tx. chain= 2


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 Ruckus-Unleashed
AP:
  ID:
    1:
```

```
           MAC Address= d4:c1:9e:35:c9:40
           Model= r610
           Approved= Yes
           Device Name= Ruckus-Unleashed
           Device Role= Master
           Description=
           Location=
           GPS=
           CERT = Normal
           Bonjour-policy=
           Bonjour-fencing=
           Group Name= System Default
           Channel Range:
             A/N= 36,40,44,48,149,153,157,161 (Disallowed= )
             B/G/N= 1,2,3,4,5,6,7,8,9,10,11 (Disallowed= )
           Radio a/n:
             Channelization= Auto
             Channel= Auto
             WLAN Services enabled= Yes
             Tx. Power= Auto
             WLAN Group Name= Default
             Call Admission Control= OFF
             Protection Mode= Auto
           Radio b/g/n:
             Channelization= Auto
             Channel= Auto
             WLAN Services enabled= Yes
             Tx. Power= Auto
             WLAN Group Name= Default
             Call Admission Control= OFF
             Protection Mode= 2
           Override global ap-model port configuration= No
           Network Setting:
             Protocol mode= IPv4-Only
             Device IP Settings= DHCP
             IP Address= 192.168.0.13
             Netmask= 255.255.255.0
             Gateway= 192.168.0.1
             Primary DNS Server= 66.90.130.101
             Secondary DNS Server= 216.82.201.11
           Mesh:
             Status= Disabled
           LLDP:
             Status = Use Parent Setting
           LAN Port:
             0:
               Interface= eth0
               Dot1x= None
               LogicalLink= Up
               PhysicalLink= Up 1000Mbps full
               Label= 10/100/1000 PoE Port1
             1:
               Interface= eth1
               Dot1x= None
               LogicalLink= Down
               PhysicalLink= Down
               Label= 10/100/1000 Port2
           PoE Mode= Auto
           802.3af PoE Tx. chain= 2

   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 d4:c1:9e:35:c9:40
AP:
  ID:
    1:
      MAC Address= d4:c1:9e:35:c9:40
      Model= r610
      Approved= Yes
      Device Name= Ruckus-Unleashed
      Device Role= Master
      Description=
      Location=
      GPS=
      CERT = Normal
      Bonjour-policy=
      Bonjour-fencing=
      Group Name= System Default
      Channel Range:
        A/N= 36,40,44,48,149,153,157,161 (Disallowed= )
        B/G/N= 1,2,3,4,5,6,7,8,9,10,11 (Disallowed= )
      Radio a/n:
        Channelization= Auto
        Channel= Auto
        WLAN Services enabled= Yes
        Tx. Power= Auto
        WLAN Group Name= Default
        Call Admission Control= OFF
        Protection Mode= Auto
      Radio b/g/n:
        Channelization= Auto
        Channel= Auto
        WLAN Services enabled= Yes
        Tx. Power= Auto
        WLAN Group Name= Default
        Call Admission Control= OFF
        Protection Mode= 2
      Override global ap-model port configuration= No
      Network Setting:
        Protocol mode= IPv4-Only
        Device IP Settings= DHCP
        IP Address= 192.168.0.13
        Netmask= 255.255.255.0
        Gateway= 192.168.0.1
        Primary DNS Server= 66.90.130.101
        Secondary DNS Server= 216.82.201.11
      Mesh:
        Status= Disabled
      LLDP:
        Status = Use Parent Setting
      LAN Port:
```

```
    0:
      Interface= eth0
      Dot1x= None
      LogicalLink= Up
      PhysicalLink= Up 1000Mbps full
      Label= 10/100/1000 PoE Port1
    1:
      Interface= eth1
      Dot1x= None
      LogicalLink= Down
      PhysicalLink= Down
      Label= 10/100/1000 Port2
  PoE Mode= Auto
  802.3af PoE Tx. chain= 2

  Channel stats:
    Available= 1,2,3,4,5,6,7,8,9,10,11
    Block=
    Available= 36,40,44,48,149,153,157,161
    Block= 165
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 Unleashed Discovery:
    Status= Disabled
  Management VLAN:
    Status= Keep AP's setting
  Auto Recovery= 30 minutes
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= 192.168.40.100
  Netmask= 255.255.255.0
  Gateway Address= 192.168.40.1
  Primary DNS= 192.168.40.1
  Secondary DNS=

Management VLAN:
  VLAN ID= 1

Country Code:
  Code= United States

Identity:
  Name= Ruckus

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

Log:
  Status= Disabled
  Address= 192.168.3.10
  Facility= local0
  Priority= emerg
  AP Facility= local0
  AP Priority= emerg

Tunnel MTU:
  Tunnel MTU= 1500

Bonjour Service:
  Status= Disabled
```

```
     Telnet Server:
       Status= Disabled

     FTP Server:
       Status= Enabled
       Anonymous Status= Enabled

     FlexMaster:
       Status= Disabled
       Address=
       Interval= 15

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

         2:
           Name= Guest Accounts
           Type= Guest
...
...
ruckus#
```

Show Performance Commands

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

show performance

Displays performance details for an AP radio or client station.

Syntax

show performance {**ap-radio2-4** |**ap-radio-5** |**ap-radio-6** | **station** } { **mac** *MAC* }

Parameters

ap-radio-2-4

Displays 2.4 GHz radio performance for an AP.

ap-radio-5

Displays AP 5 GHz radio performance for an AP.

ap-radio-6

Displays AP 6 GHz radio performance for an AP.

station

Displays performance details for a connected client station.

mac *MAC*

The MAC address of the AP or client station.

Modes

User EXEC mode

Command Output

The **show performance** command displays the following information:

Output field	Description
Radio	Specifies IEEE 802.11b, IEEE 802.11g, and IEEE 802.11n Wi-Fi standard operating on the AP radio.
MAC address	MAC address of the AP.
Estimated Capacity	Estimated capacity of the network in terms of data that can be transmitted.
Downlink	Data rate from the network to the AP.
Uplink	Data rate from the AP to the network.
RF pollution	Level of radio frequency interference in your environment.
Associated clients	The number of devices currently connected to the specified AP radio.
Other APs	The number of other RUCKUS APs detected by the specified AP. These RUCKUS APs are within the vicinity of the specified AP, and may support the same or different Wi-Fi networks.

Examples

The following example displays performance information of the 2.4 GHz AP radio.

```
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#
```

The following example displays performance information of the 5 GHz AP radio.

```
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#
```

The following example displays performance information of the specified station.

```
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#
```

History

Release version	Command history
200.16	This command was modified to include the 6 GHz radio option.

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, 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= Dedicated-Unleashed
  IP Address= 10.75.46.181
  MAC Address= 28:b3:71:2f:a1:90
  Uptime= 37d 0h 46m
  Model= R750
  Serial Number= 212002009579
  Version= 200.13.6.1 build 224

Devices Overview:
  Number of APs= 2
  Number of Client Devices= 0
  Number of Rogue Devices= 500
Usage Summary:
  Usage of 1 hr:
    Max. Concurrent Users= 0
    Bytes Transmitted= 216.10K
    Number of Rogue Devices= 500
  Usage of 24 hr:
    Max. Concurrent Users= 1
    Bytes Transmitted= 540.63M
    Number of Rogue Devices= 1154

Memory Utilization:
  Used Bytes= 170868(kB)
  Used Percentage= 10%
  Free Bytes= 1565704(kB)
  Free Percentage= 90%

Dedicated Master:
  Status= Enabled

Smart Redundancy:
  Status= Enabled
  Local Connect Status= Active
```

```
        Peer IP Address     = 10.75.46.180
        Peer Connect Status = Standby
        Shared Secret=

     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= f8:e7:1e:3a:4c:20
    Physical Link= up
    Speed= 1000Mbps
  Port  1:
    Interface= eth1
    MAC Address= f8:e7:1e:3a:4c:21
    Physical Link= down
    Speed= 100Mbps

ruckus#
```

Show Technical Support Commands

Use the following commands to display information that RUCKUS 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 Technical Support

Defaults

None.

Example

```
ruckus# show techsupport
System Overview:
  Name= Ruckus-Unleashed
  IP Address= 192.168.0.14
  MAC Address= d4:c1:9e:35:c9:40
  Uptime= 1d 1h 40m
  Model= R610
  Licensed APs= 128
  Serial Number= 941849001125
  Version= 200.9.10.4 build 110

Devices Overview:
  Number of APs= 1
  Number of Client Devices= 4
  Number of Rogue Devices= 24

Usage Summary:
  Usage of 1 hr:
    Max. Concurrent Users= 4
    Bytes Transmitted= 104.95M
    Number of Rogue Devices= 24
  Usage of 24 hr:
    Max. Concurrent Users= 5
    Bytes Transmitted= 8.27G
    Number of Rogue Devices= 38

Memory Utilization:
  Used Bytes= 202408(kB)
  Used Percentage= 43%
  Free Bytes= 268564(kB)
  Free Percentage= 57%


...
...

ruckus#
```

Show Management ACL Commands

Use the **show mgmt-acl** 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 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 WLAN Commands

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

show wlan

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

show wlan [**all**|**name**<*WORD*>]

Syntax Description

show

Display information

wlan

Display WLAN services (SSIDs) settings

all

Display all WLAN services

name <*WORD*>

Display the named WLAN only

Defaults

None.

Example

```
ruckus# show wlan all
WLAN Service:
  ID:
    1:
      NAME = Ruckus1
      Tx. Rate of Management Frame(2.4GHz) = 2.0Mbps
      Tx. Rate of Management Frame(5GHz)   = 6.0Mbps
      Beacon Interval = 100ms
      SSID = Ruckus1
      Description = Ruckus1
      Type = Standard Usage
      Authentication = open
      Encryption = wpa2
      Algorithm = aes
      Passphrase = secretpassphrasegoeshere
      FT Roaming = Disabled
      802.11k Neighbor report = Disabled
      Web Authentication = Disabled
      Authentication Server = Disabled
      Accounting Server = Disabled
      Called-Station-Id type = wlan-bssid
      Tunnel Mode = Disabled
      DHCP relay = Disabled
      Max. Clients = 100
      Isolation per AP = Disabled
      Isolation across AP = Disabled
      Zero-IT Activation = Enabled
      Load Balancing = Disabled
      Band Balancing = Disabled
      Wifi6 = Enabled
```

```
        Service = Enabled
        Dynamic PSK = Enabled
        Dynamic PSK Passphrase Length =
        Dynamic PSK Expire Time = unlimited
        Dynamic PSK Validity Period =
        Limit Dynamic PSK = Disabled
        Auto-Proxy configuration:
          Status = Disabled
        Inactivity Timeout:
            Status = Disabled
        VLAN-ID = 1
        Dynamic VLAN = Disabled
        Closed System = Disabled
        Https Redirection = Disabled
        OFDM-Only State = Disabled
        Multicast Filter State = Disabled
        802.11d State = Disabled
        Force DHCP State = Disabled
        Force DHCP Timeout = 0
        DHCP Option82:
            Status = Disabled
            Option82 sub-Option1 = Disabled
            Option82 sub-Option2 = Disabled
            Option82 sub-Option150 = Disabled
            Option82 sub-Option151 = Disabled
        Ignore unauthorized client statistic = Disabled
        STA Info Extraction State = Enabled
        BSS Minrate = Disabled
        DTIM period = 1
        Directed MC/BC Threshold = 5
        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 = No ACLS
        Proxy ARP = Disabled
        Device Policy = No ACLS
        Vlan Pool = No Pools
        Role based Access Control Policy = Disabled
        SmartRoam = Disabled  Roam-factor = 1
        Allow List = No ACLS
        Application Recognition & Control = Disabled
        Apply ARC Policy = NO POLICY
        Wlan Bind = all
        Client Flow Data Logging = Disabled
        Client Connection Data = Disabled


    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 Allowlist Commands

Use the **show allowlist** commands to display client isolation allowlists that have been added to the controller.

show allowlist all

To display all allowlists that have been added to the controller and their settings, use the following command:

show allowlist all

Syntax Description

show

Display information

allowlist

Display allowlist information

all

All allowlists

Defaults

None.

Example

```
ruckus# show allowlist all
Allow Lists:
  ID:
    1:
      Name= printer allowlist
      Description= printer
      Rules:
        1:
          Description= printer
          MAC = 12:34:56:78:90:00
          IP Address = 192.168.4.10

ruckus#
```

show allowlist name

To display a specified allowlist that has been added to the controller by name, use the following command:

show allowlist name *WORD*

Syntax Description

show

Display information

allowlist

Display allowlist information

name *WORD*

Specify the name of the allowlist

Defaults

None.

Example

```
ruckus# show allowlist name "printer allowlist"
Allow Lists:
  ID:
    1:
      Name= printer allowlist
      Description= printer
      Rules:
        1:
          Description= printer
          MAC = 12:34:56:78:90:00
          IP Address = 192.168.4.10

ruckus#
```

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 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 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= Hotspot 1
      WISPr Smart Client Support:
        Status= None
      Login Page Url= http://192.168.1.12/login.htm
      Start Page= redirect to the URL that the user intends to visit
      Session Timeout:
        Status= Disabled
      Grace Period:
        Status= Disabled
      Intrusion Prevention= Enabled
      Authentication Server= Local Database
      Accounting Server:
        Status= Disabled
      Isolation per AP = Disabled
      Isolation across AP = Disabled
      Allow List = No ACLS
      Location ID=
      Location Name=
      Walled Garden 1= 1.1.1.1
      IPv4 Rules:

      IPv6 Rules:


ruckus#
```

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 "Hotspot 1"
Hotspot:
  ID:
    1:
      Name= Hotspot 1
      WISPr Smart Client Support:
        Status= None
      Login Page Url= http://192.168.1.12/login.htm
      Start Page= redirect to the URL that the user intends to visit
      Session Timeout:
        Status= Disabled
      Grace Period:
        Status= Disabled
      Intrusion Prevention= Enabled
      Authentication Server= Local Database
      Accounting Server:
        Status= Disabled
      Isolation per AP = Disabled
      Isolation across AP = Disabled
      Allow List = No ACLS
      Location ID=
      Location Name=
      Walled Garden 1= 1.1.1.1
      IPv4 Rules:

      IPv6 Rules:


ruckus#
```

Show Guest Policy Commands

Use the following commands to display guest access services.

show guest-access-service

To display a list of guest access services or a specific service, use the following command:

show guest-access-service [**all** | **name** *WORD*]

Example

```
ruckus# show guest-access all
Guest Access:
  Name = guestpolicy1
  Onboarding Portal:
    Aspect = Guest pass and ZeroIT
  Authentication:
    Mode = Use Guest Pass and Social login authentication
  Title = hello
  Terms of Use:
    Status = Disabled
  Redirection:
    Mode = To the URL that the user intends to visit
  Restricted Subnet Access:
      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:
      Rules:
        1:
          Description=
          Type= Deny
          Destination Address= local
          Destination Port= Any
          Protocol= Any
          ICMPv6 Type= Any

  ruckus#
```

Show Hotspot 2.0 Operator Commands

Use the following commands to display Hotspot 2.0 Operators.

show hs20op

To display a list of Hotspot 2.0 operators, use the following command:

show hs20op [all|name *WORD*]

Example

```
ruckus# show hs20op all
```

Show Hotspot 2.0 Service Provider Commands

Use the following commands to display Hotspot 2.0 Service Providers.

show hs20sp

To display a list of Hotspot 2.0 service providers, use the following command:

show hs20sp [all|name *WORD*]

Example

```
ruckus# show hs20sp all
```

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, 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
      Unleashed Administration:
        Status= Disallowed
      Allow All WLANs:
        Mode= Allow access to all WLANs
      Access Control Policy= Disallowed


ruckus#
```

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
      Unleashed Administration:
        Status= Disallowed
      Allow All WLANs:
        Mode= Allow access to all WLANs
      Access Control Policy= Disallowed

ruckus#
```

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 *WORD*

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 mesh information, 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-951608000220
  Mesh Passphrase= bzj9Y0kEpkxOPzPXyKqLrJHZSAAnbtfaTm7Ebh6qps24PFPcc5MtCiijGGwFZBG
  Mesh Radio Option= 5G
  Mesh Uplink Selection Algorithm = default(static)
  Mesh Hop Detection:
    Status= Disabled
  Mesh Downlinks Detection:
    Status= Disabled
  Tx. Rate of Management Frame=  2Mbps
  Beacon Interval= 200ms
  Zero-Touch-Mesh status= Enabled
Zero Touch Mesh Pre-Approved Serial Number List:
serial number = 921802014959, approved = 0, time = 0, id = 1
serial number = 441e981cf0d0, approved = 0, time = 0, id = 2
serial number = 4f1e681cf3f0, approved = 0, time = 0, id = 3
serial number = c41e781bd7c0, approved = 0, time = 0, id = 4

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-951608000220):
  Root Access Points= d4:c1:9e:35:c9:50
    Signal (dB) Downlink=  / Uplink=
    Description=
    Channel= 36 (11ac)
    IP Address= 192.168.0.3
    Mesh Access Points= 44:1e:98:1b:f0:d0
      Signal (dB) Downlink= 44 / Uplink= 36
      Description=
      Channel= 36
      IP Address= 192.168.0.10

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

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 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

show guest-passes

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 guest-access-generation

Display generation information for guest access.

Examples

```
ruckus# show guest-access-generation
  Authentication Server: radius1
  Force HTTPS Redirection: Disabled
ruckus#
```

show portal-auth-generation

Display generation information for portal authentication.

Examples

```
ruckus# ruckus# show portal-auth-generation
  Force DNS server: 192.168.40.10
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

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

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

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

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 Application Policy Commands

Use the following commands to display application policies, user-defined applications and application port-mapping settings.

show app-policy

show app-policy

Syntax Description

show

Display information

app-policy

Display application policies

Defaults

None.

Example

```
ruckus# show app-policy
Application Policy:
  ID:
ruckus#
```

show user-app-ip

show user-app-ip

Syntax Description

show

Display information

user-app-ip

Display IP-based user defined applications

Defaults

None.

Example

```
ruckus# show user-app-ip
User defined application hasn't been found.
ruckus#
```

show user-app-port

show user-app-port

Syntax Description

show

Display information

license

Display port-based user defined applications

Defaults

None.

Example

```
ruckus# show user-app-port
Application based on port hasn't been found.
ruckus#
```

show wificalling

Syntax Description

show

Display information.

wificalling

Display the current Wi-Fi Calling settings.

Example

```
ruckus# show wificalling
    1:
      WIFI Calling Carrier Name: AT&T
      WIFI Calling Description: AT&T
      WIFI Calling Priority: 3
          WIFI Calling Domains: internal.att.com
          WIFI Calling IP address:129.192.166.10
    2:
      WIFI Calling Carrier Name: profile1
      WIFI Calling Priority: 1
          WIFI Calling Domains: Tmobile
          WIFI Calling IP address:10.10.100.100
ruckus#
```

show url-filtering

show url-filtering

Syntax Description

show

> Display information

url-filtering

> Display the current URL filtering settings.

Example

```
ruckus# show url-filtering
Url Filtering Profiles:
    1:
      Url Name: Profile 1
      Filter Type: CLEAN_AND_SAFE
      Number of Blocked Categories: 25
      Blocked Categories:
              Abortion
              Abused Drugs
              Adult and Pornography
              Bot Nets
              Confirmed SPAM Sources
              Cult and Occult
              Dating
              Dead Sites
              Gambling
              Gross
              Hacking
              Hate and Racism
              Illegal
              Keyloggers and Monitoring
              Malware Sites
              Marijuana
              Nudity
              Pay to Surf
              Phishing and Other Frauds
              Proxy Avoidance and Anonymizers
              SPAM URLs
              Spyware and Adware
              Unconfirmed SPAM Sources
              Violence
              Weapons
      Blocklist-Domains: Not Configured
      Allowlist-Domains: Not Configured
      Google Safe Search: Disabled
      YouTube Safe Search: Disabled
      Bing Safe Search: Disabled
    2:
      Url Name: Profile 2
      Filter Type: CLEAN_AND_SAFE
      Number of Blocked Categories: 25
      Blocked Categories:
              Abortion
              Abused Drugs
              Adult and Pornography
              Bot Nets
              Confirmed SPAM Sources
              Cult and Occult
              Dating
              Dead Sites
              Gambling
              Gross
              Hacking
              Hate and Racism
              Illegal
              Keyloggers and Monitoring
              Malware Sites
```

```
            Marijuana
            Nudity
            Pay to Surf
            Phishing and Other Frauds
            Proxy Avoidance and Anonymizers
            SPAM URLs
            Spyware and Adware
            Unconfirmed SPAM Sources
            Violence
            Weapons
    Blocklist-Domains:
            blockthiswebsite.com
    Allowlist-Domains: Not Configured
    Google Safe Search: Disabled
    YouTube Safe Search: Disabled
    Bing Safe Search: Disabled
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#
```

Show RADIUS Statistics Commands

Use the following commands to display RADIUS statistics or to reset RADIUS statistics.

show radius-statistics

To display a list of RADIUS server statistics, use the following command:

show radius-statistics [**server-all** | **server-name** *WORD*] | [**wlan-all** | **wlan-name** *NAME*] [**latest-ten-min** | **latest-one-hour** | **latest-one-day**]

Syntax Description

show radius-statistics

Display list of RADIUS server statistics.

server-all

Display statistics for all servers. (Default: recorded from power on.)

server-name *WORD*

Display statistics for the specified server. (Default: recorded from power on.)

wlan-all

Display statistics for all WLANs. (Default: recorded for the last day.)

wlan-name *NAME*

Display statistics for the specified WLAN. (Default: recorded for the last day.)

latest-ten-min

Display statistics for the last 10 minutes.

latest-one-hour

Display statistics for the last hour.

latest-one-day

Display statistics for the last day.

reset radius-statistics

To reset RADIUS statistics, use the following command:

reset radius-statistics [**server-all** | **server-name** *WORD*] [**master** | **standby**] [**latest-ten-min** | **latest-one-hour** | **latest-one-day**]

Syntax Description

reset radius-statistics

Reset RADIUS server statistics.

server-all

Reset statistics for all servers to zero. (Default: recorded from power on.)

server-name *WORD*

Reset statistics for the specified server to zero. (Default: recorded from power on.)

wlan-all

Reset statistics for all WLANs. (Default: recorded for the last day.)

wlan-name *NAME*

Reset statistics for the specified WLAN. (Default: recorded for the last day.)

master

Reset statistics of the master server to zero.

standby

Reset statistics of the standby server to zero.

latest-ten-min

Reset statistics recorded for the last 10 minutes

latest-one-hour

Reset statistics recorded for the last hour

latest-one-day

Reset statistics recorded for the last day

Show Load Balancing Commands

Use the following commands to display AP load balancing information.

show load-balance

To display AP load balancing information, use the following command:

show load-balance

Example

```
ruckus# show load-balance
*** Show AP load balance
Radio---Enable--Scan--ActThresh---AdjThresh---WeakBypass---StrongBypass---NewActTrigger---Headroom
 2GHz      0   2000         10         50           33            55             3              3
 5GHz      0   2000         10         43           35            55             3              3
----MAC Address----Cli-New-Lim---Allow-----Fallbk----Adjacent 2-GHz Radios [MacAdrs FwdRssi RevRssi
SumRssi]
 c4:10:8a:1f:d1:f0   1   0    0 1000000000 0000000000
 c0:c5:20:3b:91:f0   2   0    0 1000000000 0000000000
----MAC Address----Cli-New-Lim---Allow-----Fallbk----Adjacent 5-GHz Radios [MacAdrs FwdRssi RevRssi
SumRssi]
 c4:10:8a:1f:d1:f0   0   0    0 1000000000 0000000000
 c0:c5:20:3b:91:f0   1   0    0 1000000000 0000000000
ruckus#
```

Show Station Rename Commands

Use the **show sta-rename** command to display the current renamed station list.

show sta-rename

To display the current renamed station list, use the following command:

show sta-rename

Example

```
ruckus# show sta-rename
Displays sta rename list.
    MAC Address= 6C:AA:B3:00:00:A0
    rename= my-iphone


All sta rename number: 1
```

Show Station Favorite Commands

Use the **show sta-favorite** command to display the current favorite station list.

show sta-favorite

To display the current favorite station list, use the following command:

show sta-favorite

Example

```
ruckus# show sta-favorite
Displays sta favorite list.
    MAC Address= aa:aa:aa:aa:aa:aa
    MAC Address= bb:bb:bb:bb:bb:bb


All sta favorite number: 2
```

Configuring Master Settings

Configuration Commands Overview

This section describes the commands that you can use to configure Unleashed 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. To save your configuration changes and exit the **config** context, use the end or exit command. To discard your changes and exit the **config** context, use the abort or quit command.

Some sub-contexts within the **config** context do not allow the use of the abort or quit commands; you must save your changes and exit the sub-context. Many commands offer a corresponding "no" command to undo your configuration changes (for example, use "no wlan" to delete a WLAN).

help

Shows available commands.

history

Shows a list of previously run commands.

abort

Exits the **config** context without saving changes. Some contexts do not allow **abort**, you must save your changes to exit the context (**end** or **exit**).

end

Saves changes, and then exits the **config** context.

exit

Saves changes, and then exits the **config** context.

quit

Exits the **config** context without saving changes. Some contexts do not allow quit, you must save your changes to exit the context (**end** or **exit**).

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 login settings.

Example

```
ruckus(config)# show admin
Administrator Name/Password:
  Name= admin
  Password= ********
  Authenticate:
    Mode= Authenticate using the admin name and password

ruckus(config)#
```

show mgmt-acl

Displays a list of all management access controls.

show static-route

Displays a list of all static route entries.

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 allowlist

Displays a list of client isolation allow lists.

show prece

Displays a list of Precedence Policies.

Defaults

Name= Default

Description= None

Attribute=vlan

- Order = AAA,Device Policy,WLAN

Attribute = rate-limit

- Order = AAA,Device Policy,WLAN

Example

```
ruckus(config)# show prece
Precedence Policy:
  ID:
    1:
      Name= Default
      Description=
      Rules:
        1:
          Description=
          Attribute = vlan
          Order = AAA,Device Policy,WLAN
        2:
          Description=
          Attribute = rate-limit
          Order = AAA,Device Policy,WLAN


ruckus(config)#
```

show dvcpcy

Displays a list of Device Policies.

show user-app-ip

Displays the IP-based user-defined applications.

Example

```
ruckus(config)# show user-app-ip
User defined application hasn't been found.
ruckus(config)#
```

show user-app-port

Displays the user-defined port-based application settings.

Example

```
ruckus(config)# show user-app-port
Application based on port hasn't been found.
ruckus(config)#
```

show user-app-port

Displays the user-defined application port mapping settings.

show url-filtering

Displays the URL filtering profiles.

show wificalling

To display Wi-Fi Calling profiles, use the following command:

show wificalling

Example

```
ruckus(config)# show wificalling
    1:
      WIFI Calling Carrier Name: AT&T
      WIFI Calling Description: AT&T
      WIFI Calling Priority: 3
          WIFI Calling Domains: internal.att.com
          WIFI Calling IP address:129.192.166.10
    2:
      WIFI Calling Carrier Name: profile1
      WIFI Calling Priority: 1
          WIFI Calling Domains: Tmobile
          WIFI Calling IP address:10.10.100.100
ruckus(config)#
```

show load-balancing

Displays information about Load balancing.

Example

```
ruckus(config)# show load-balancing
Load Balancing:
  Radio 0:
      Status= Disabled
      AdjacentThreshold= 50
      WeakBypass= 33
      StrongBypass= 55
      ActivationThreshold= 10
      NewTrigger= 3
      Headroom= 3

  Radio 1:
      Status= Disabled
      AdjacentThreshold= 43
      WeakBypass= 35
      StrongBypass= 55
      ActivationThreshold= 10
      NewTrigger= 3
      Headroom= 3


ruckus(config)#
```

show wlan

Displays a list of all WLAN services (Names).

show wlan-group

Displays a list of existing WLAN groups.

Example

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

ruckus(config)#
```

show role

Displays a list of roles.

show user

Displays a list of users.

show hotspot

Displays a list of hotspot entries.

show guest-access-service

To display a list of guest access services, use the following command:

show guest-access-service

show guest-access-generation

To display generation information for guest access, use the following command:

show guest-access-generation

Example

```
ruckus(config)# show guest-access-generation
  Authentication Server: Local Database
  Force HTTPS Redirection: Disabled
ruckus(config)#
```

show portal-auth-generation

To display generation information for portal authentication, use the following command:

show portal-auth-generation

Example

```
ruckus(config)# show portal-auth-generation
  Force DNS server: Disabled
  Force Web Portal HTTPS Redirection: Enabled
ruckus(config)#
```

show ap-group

To display all or specified AP groups, use the following command:

show ap-group [**all** | **name** *WORD*]

show location-services

Displays a list of configured location services.

show sta-rename

Displays a list of renamed stations.

show sta-favorite

Displays a list of favorite stations.

show hs20op

Displays the list of hotspot 2.0 operator settings.

show hs20sp

Displays a list of hotspot 2.0 service provider settings.

show mdnsproxyrule

To display Mdnsproxy rules, use the following command:

show mdnsproxyrule *ID-From ID-to*

show mdnsproxy

To display Mdnsproxy status, use the following command:

show mdnsproxy *ID-From ID-to*

show bonjour-policy

To display Bonjour policy rules, use the following command:

show bonjour-policy *name*

show bonjour-fencing

To display Bonjour Fencing rules, use the following command:

show bonjour-fencing *name*

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 context, type **help** or **?**.

aaa

Use the following command to configure an AAA server entry and enter the config-aaa context:

aaa *WORD*

Syntax Description

abort

Exits the config-aaa context without saving changes.

end

Saves changes, and then exits the config-aaa context.

exit

Saves changes, and then exits the config-aaa context.

quit

Exits the config-aaa context without saving changes.

name *WORD*

Sets the AAA server name.

show

Displays a list of available AAA servers.

CaseSensitive

Sets the 'CaseSentitive' value of AD/LDAP server to 'enabled'.

type

Sets the type of AAA server.

type ad

Sets the AAA server type to 'Active Directory'.

type ldap

Sets the AAA server type to 'LDAP'.

type ad-802.1x

Sets the AAA server type to 'Active Directory For 802.1x '.

type radius-auth

Sets the AAA server type to 'RADIUS'.

type tacplus-auth

Sets the AAA server type to 'TACPLUS'.

type radius-acct

Sets the AAA server type to 'RADIUS Accounting'.

radius-encryption

Sets the AAA server encryption type.

radius-encryption tls

Sets the AAA server encryption type to 'TLS'.

auth-method pap

Sets the authentication method to PAP.

auth-method chap

Sets the authentication method to CHAP.

ip-addr *IP-ADDR*

Sets the AAA server's IP/IPv6 address.

port *PORT-NUM*

Sets the AAA server's port.

tacplus-service *WORD*

Sets TACPLUS service name with length (1-64 bytes).

domain-name *WORD*

Sets the windows/base domain name.

domainServer-deviceName*WORD*

Sets the domain server device name.

no radius-encryption

Disables the AAA server encryption.

no ad-global-catalog

Disables global catalog support.

no grp-search

Disables group attribute lookup support.

no encryption-TLS

Disable the TLS Encryption

no backup

Disables the backup function.

ad-global-catalog

Enables global catalog support.

grp-search

Enables group attribute lookup support.

admin-dn *WORD*

Sets the admin domain name.

admin-password *WORD*

Sets the admin password.

key-attribute *WORD*

Sets the LDAP key attribute.

search-filter *WORD*

Sets the LDAP search filter.

radius-secret *WORD*

Sets the AAA server's shared secret.

tacplus-secret *WORD*

Sets the TACPLUS server's shared secret.

encryption-TLS

Enables the TLS Encryption

backup

Enables the backup function.

backup-ip-addr *IP-ADDR*

Sets the backup AAA server's IP/IPv6 address.

backup-port *PORT-NUM*

Sets the backup AAA server's port.

backup-radius-secret *WORD*

Sets the backup AAA server's shared secret.

request-timeout *NUMBER*

Sets the failover request timeout (2~20 seconds).

retry-count *NUMBER*

Sets the failover retry count (2~10 times).

consecutive-drop-packet *NUMBER*

Sets the number of consecutive dropped packet (range:1~10 , default is 1).

reconnect-primary-interval *NUMBER*

Sets the failover re-connect to primary interval (1~86400 minutes).

Example

```
ruckus(config)# aaa activedir
The AAA server 'activedir' has been created. 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)# ip-addr 192.168.10.40
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-aaa)# show
AAA:
  ID:
    :
      Name= activedir
      Type= Active Directory
      IP Address= 192.168.10.40
      Port= 389
      Windows Domain Name=
      Global Catalog= Disabled
      Admin DN=
      Admin Password=
      Group Search= Enabled
      encryption-TLS = Disabled

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

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

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

super

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

sp-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)#
```

show

To view the current admin login and authentication settings, use the following command:

show

Example

```
ruckus(config-admin)# show
Administrator Name/Password:
  Name= admin
  Password= ********
  Authenticate:
    Mode= Authenticate using the admin name and password

ruckus(config-admin)#
```

Configure Access Points Commands

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

bonjour-gateway

To bind a bonjour gateway policy to this AP, use the following command:

bonjour-gateway *WORD*

Example

```
ruckus(config-ap)# bonjour-gateway bonjour1
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-ap)#
```

no bonjour-gateway

To unbind a bonjour gateway policy, use the following command:

no bonjour-gateway

Example

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

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

Example

```
ruckus(config-ap)# ip enable mode dhcp
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

status-lacp

To enable or disable LACP, use the following command:

status-lacp [**enable** | **disable**]

Defaults

Disabled.

Example

```
ruckus(config-ap)# status-lacp enable
ruckus(config-ap)#
```

no status-lacp-override

To disable override of AP group LACP settings, use the following command:

no status-lacp-override

Example

```
ruckus(config-ap)# no status-lacp-override
ruckus(config-ap)#
```

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

external-antenna

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

external-antenna [**2.4G**|**5G**][**enable**|**disable**]

Syntax Description

2.4G

Configure external 2.4GHz antenna

5G

Configure external 5GHz antenna

enable|**disable**

Enable/disable external antenna

Defaults

Varies by AP model.

no external-antenna-override

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

no external-antenna-override

spectra-analysis 2.4GHz

To enable or disable the spectrum analysis feature for this radio, use the following command:

spectra-analysis 2.4GHz [**enable** | **disable**]

spectra-analysis 5GHz

To enable or disable the spectrum analysis feature for this radio, use the following command:

spectra-analysis 5GHz [**enable** | **disable**]

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

cband-license

To override the group configuration and enable or disable 5.8 GHz radio full power for this device, use the following command:

cband-license [**enable** | **disable**]

Defaults

Disabled.

Example

```
ruckus(config-ap)# cband-license enable
Model r610 doesn't support to configure cband-license.
ruckus(config-ap)#
```

no cband-license-override

To disable the override of the 5.8 GHz Channels License for this AP, use the following command:

no cband-license-override

Defaults

Disabled.

Example

```
ruckus(config-ap)# no cband-license override
Model r610 doesn't support to configure cband-license.
ruckus(config-ap)#
```

radio-band

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

radio-band *WORD*

Syntax Description

radio-band

Configure radio band mode

WORD

Set to 2.4 or 5 GHz radio mode

Usage Guidelines

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

Example

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

no radio-band-override

To disable the AP radio band override, 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)#
```

lldp

To enable, disable or configure the AP's Link Layer Discover Protocol settings, use the following lldp commands from within the config-ap context.

Syntax Description

lldp

Configure LLDP settings.

enable

Enable LLDP with current settings.

disable

Disable LLDP with current settings.

interval *NUMBER*

Set packet transmit interval in second(s).

holdtime *NUMBER*

Set amount of time receiving device should retain the information.

ifname eth *NUMBER*

Enter the AP port number.

mgmt enable

Enable LLDP management IP address of the AP.

mgmt disable

Disable LLDP management IP address of the AP.

Example

```
ruckus(config-ap)# lldp enable
ruckus(config-ap)#
```

no lldp-override

To disable the AP's LLDP override settings (use parent settings), use the following command:

no lldp-override

Example

```
ruckus(config-ap)# no lldp-override
ruckus(config-ap)#
```

power-mode

To set the PoE mode of the AP, use the following command:

power-mode *<WORD>*

Syntax Description

power-mode

Set the PoE power mode.

auto

Set the PoE power mode to auto.

802.3af

Set the PoE power mode to 802.3af.

802.3at

Set the PoE power mode to 802.3at.

802.3bt5

Set the PoE power mode to 802.3bt5.

802.3bt6

Set the PoE power mode to 802.3bt6.

802.3bt7

Set the PoE power mode to 802.3bt7.

Example

```
ruckus(config-ap)# power-mode 802.3af
ruckus(config-ap)#
```

no power-mode-override

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

no power-mode-override

802.3af-txchain

To set the number of 2.4 GHz radio transmit chains in 802.3af PoE power mode, use the following command:

802.3af-txchain *WORD*

Syntax Description

802.3af-txchain

Set the number of 2.4 GHz radio transmit chains in 802.3af power mode.

1

Set the number of tx chains to 1.

2

Set the number of tx chains to 2.

4

Set the number of tx chains to 4.

Example

```
ruckus(config-ap)# 802.3af-txchain 2
ruckus(config-ap)#
```

no 802.3af-txchain-override

To disable the override of the 2.4GHz radio transmit chains in 802.3af PoE mode, use the following command:

no 802.3af-txchain-override

Example

```
ruckus(config-ap)# no 802.3af-txchain-override
ruckus(config-ap)#
```

Radio 2.4, 5, 6 GHz Commands

Use the **radio 2.4**, **radio 5**, or **radio 6** commands to configure the 2.4, 5, or 6 GHz radio settings, respectively, on an AP. These commands allow you to adjust the settings of each radio frequency band independently.

radio (AP)

Configures the 2.4, 5, and 6 GHz radio settings independently on an AP.

Syntax

radio { **2.4** | **5** | **6** } [**channelization** { **auto** | *number* }] [**channel** { **auto** | *number* }] [**tx-power** { **auto** | **full** | **min** | *1-10* }] [**wlan-group** *group_name*] [**wlan-service** { *enable* |*disable* }] [**admission-control** *value*] [**channel range** *number-list*]

no radio { **2.4** | **5** | **6** }[**channelization** { **auto** | *number* }] [**channel** { **auto** | *number* }] [**tx-power** { **auto** | **full** | **min** | *1-10* }] [**wlan-group** *group_name*] [**wlan-service** { *enable* |*disable* }] [**admission-control** *value*] [**channel range** *number-list*]

Command Default

The default radio setting values are:

Parameter	Value
channelization	Auto
channel	Auto
tx-power	Auto
wlan-group	Default
wlan-service	Enabled
wlan-service-override	Disabled
tx-power	Auto
admission-control	Disabled
spectralink-compatibility	Disabled

Parameters

2.4

Configures the 2.4 GHz radio.

5

Configures the 5 GHz radio.

6

Configures the 6 GHz radio. This option is supported only in tri-band APs.

channelization { **auto** | *number* }

AP channel width. For the 2.4 GHz radio, valid values are auto, 20, or 40 MHz. For the 5 GHz radio, valid values are auto, 20, 40, and 80 MHz. For the 6 GHz radio, valid values are auto, 20, 40, 80, 160, and 320 MHz.

channel { **auto** | *number* }

AP channel. Valid values are auto or a specific channel number. From 1 through 233 for 20 MHz, or from 1 through 229 for 40 MHz, or from 1 through 221 for 80, 160, or 320 MHz channels.

tx-power { **auto** | **full** | **min** | **num** *1-10* }

AP transmit power. Valid values are auto, full, min, or a specific dB value in the range of -1 through -10.

admission-control *value*

Call admission control airtime usage limit (as a precentage).

channel range *number-list*

Channels allowed.

wlan-group *group_name*

WLAN group name.

wlan-service { **enable** | **disable** }

Enable WLAN service on this radio

Modes

AP configuration mode

Usage Guidelines

The *6 GHz* radio can be configured only on the tri-band APs.

The **no** form of the command removes the configured values for the radios, reverting to the default configuration settings.

Examples

The following example configures the 2.4 GHz radio settings globally for all APs.

```
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)#
```

History

Release version	Command history
200.16	This command was modified to include the 6 GHz radio setting.

show

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

show

Example

```
ruckus(config)# ap c0:8a:de:21:a8:10
The AP 'c0:8a:de:21:a8:10' has been loaded. To save the AP, type 'end' or 'exit'.
ruckus(config-ap)# show
AP:
  ID:
    1:
```

```
          MAC Address= c0:8a:de:21:a8:10
          Model= zf7982
          Approved= Yes
          Device Name= RuckusAP
          Description=
          Location=
          GPS=
          CERT = Complex
          Bonjour-policy=
          Bonjour-fencing= Disabled
          Group Name= System Default
          Channel Range:
            A/N= 36,40,44,48,149,153,157,161 (Disallowed= )
            B/G/N= 1,2,3,4,5,6,7,8,9,10,11 (Disallowed= )
          Radio a/n:
            Channelization= Auto
            Channel= Auto
            WLAN Services enabled= Yes
            Tx. Power= Auto
            WLAN Group Name= Default
            Call Admission Control= OFF
            Protection Mode= Auto
          Radio b/g/n:
            Channelization= Auto
            Channel= Auto
            WLAN Services enabled= Yes
            Tx. Power= Auto
            WLAN Group Name= Default
            Call Admission Control= OFF
            Protection Mode= 2
          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= 10.10.3.51
            Netmask= 255.255.0.0
            Gateway= 10.10.0.1
            Primary DNS Server= 10.10.0.1
            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= Disabled
          LLDP:
            Status = Use Parent Setting
          Venue Name List:
          LAN Port:
            0:
              Interface= eth0
              Dot1x= None
              LogicalLink= Up
              PhysicalLink= Up 100Mbps full
              Label= 10/100/1000 PoE LAN1
            1:
              Interface= eth1
              Dot1x= None
              LogicalLink= Down
              PhysicalLink= Down
              Label= 10/100/1000 LAN2

    ruckus(config-ap)#
```

Mesh Commands

Use the following commands to configure the AP's mesh-related settings.

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.

Examples

```
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)#

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

maxhops

To set the maximum mesh hops for the AP (0-3), use the following command:

maxhops *<NUMBER>*

Example

```
ruckus(config-ap)# maxhops 3
The command was executed successfully. To save the changes, type 'end' or 'exit'.
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

Syntax Description

port-setting
> Configure AP port settings

lan *NUMBER{Arguments}*
> Configure the AP LAN port

no lan *NUMBER*
> Disable the AP LAN port

uplink *WORD*
> Set the AP port to use the specified type (trunk, access or general)

rate-uplink *NUMBER*
> Set the uplink rate limiting value, ranging from 0 through 1000

rate-downlink *NUMBER*
> Set the downlink rate limiting value, ranging from 0 through 1000

untag *NUMBER*
> Set the AP port to use the specified VLAN ID (1-4094)

member *NUMBER*
> Set the AP port to use the specified members (1-4094)

opt82 [**enabled**|**disabled**]
> Enable the AP port DHCP Option 82 settings

tunnel[**enabled**|**disabled**]
> Enable the AP port tunnel settings

guest-vlan *NUMBER*
> Set the AP port to use the specified guest VLAN ID (1-4094)

dvlan[**enabled**|**disabled**]
> Enable the AP port dynamic VLAN settings

no dot1x *authsvracctsvrmac-auth-bypass*
> Disable authentication server, accounting server, or MAC auth bypass for the AP's 802.1X settings

dot1x *authsvracctsvrmac-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

dot1x supplicant [**username** | **password**]*WORD*

Set the username/password for AP 802.1X supplicant

dot1x supplicant mac

Set the username and password to use AP MAC address for AP 802.1X supplicant

Defaults

Enable LAN: Yes

LAN Type: trunk

Untag ID: 1

Members: 1-4094

Guest VLAN: Disabled

Dynamic VLAN: Disabled

802.1X: disabled

DHCP opt82: Disabled

Tunnel= Disabled

MLD Snooping: Disabled

IGMP Snooping: Enabled

Example

```
ruckus(config-ap)# port-setting
ruckus(config-ap-model)# lan 1 uplink trunk
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
            Tunnel= 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
            Tunnel= Disabled
```

```
             MLD Snooping= Disabled
             IGMP Snooping= Enabled

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

abort

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

abort

end

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

end

exit

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

exit

quit

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

quit

show

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

show

Example

```
ruckus(config)# ap 04:4f:ab: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
          Tunnel= 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
            Tunnel= 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

uplink *WORD*

Sets the AP port to use the specified type(trunk,access or general).

untag *NUMBER*

Sets the AP port to use the specified VLAN ID(1-4094) or none.

member *NUMBER*

Sets the AP port to use the specified members(1-4094).

opt82

Sets the AP port DHCP Option 82.

tunnel

Sets the AP port tunnel.

guest-vlan *NUMBER*

Sets the AP port to use the specified guest VLAN ID(1-4094).

dvlan

Sets the AP port dynamic VLAN.

dot1x

Sets the AP port 802.1X.

Defaults

Enable LAN = Yes

LAN Type= trunk

Untag ID= 1

Members= 1-4094

Guest VLAN=

Enable Dynamic VLAN= Disabled

802.1X= disabled

DHCP opt82= Disabled

Tunnel= Disabled

MLD Snooping= Disabled

IGMP Snooping= 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 7025/7055: Trunk

For 7025/7055 LAN 5: Trunk

For 7025/7055 LAN 1-LAN 4: Access

Example

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

lan rate-uplink

To set rate limiting on a port, use the following command:

lan *NUMBER* **rate-uplink** *NUMBER*

> **NOTE**
> The **rate-uplink** command is supported only for H550/H350 or H320/H510 in Gateway model.

Syntax Description

lan

Configure a specific port

NUMBER

Configure this port

rate-uplink

Set the uplink rate limiting

NUMBER

Enter the rate limiting to {NUMBER} Mbps, valid range is from 0 to 1000.

Defaults

None.

Example

```
ruckus(config-ap-model)# lan 1 rate-uplink 200
ruckus(config-ap-model)# show
PORTS:
    LAN ID:
          1:
            Rate Uplink= 200
ruckus(config-ap-model)#
```

lan rate-downlink

To set rate limiting on a port, use the following command:

lan *NUMBER* **rate-downlink** *NUMBER*

> **NOTE**
> The **rate-downlink** command is supported only for H550/H350 or H320/H510 in Gateway model.

Syntax Description

lan

Configure a specific port

NUMBER

Configure this port

rate-downlink

Set the downlink rate limiting

NUMBER

Enter the rate limiting to {NUMBER} Mbps, valid range is from 0 to 1000.

Defaults

None.

Example

```
ruckus(config-ap-model)# lan 1 rate-downlink 300
ruckus(config-ap-model)# show
PORTS:
    LAN ID:
         1:
             Rate Downlink= 300
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 2 member 1-10,100,200
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
            Tunnel= Disabled
            MLD Snooping= Disabled
            IGMP Snooping= Enabled
        2:
            Enable LAN = Yes
            LAN Type= general
            Untag ID= 1
            Members= 1-10,100,200
            Guest VLAN=
            Enable Dynamic VLAN= Disabled
            802.1X= disabled
            DHCP opt82= Disabled
            Tunnel= Disabled
            MLD Snooping= Disabled
```

```
              IGMP Snooping= Enabled

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 tunnel

To enable or disable Ethernet port tunnel mode for the port, use the following command:

lan *NUMBER* **tunnel** [**enabled** | **disabled**]

Syntax Description

tunnel

Enable or disable port tunnel mode

enabled

Enable tunnel mode

disabled

Disable tunnel mode

Defaults

Disabled

Example

```
ruckus(config-ap-model)# lan 1 tunnel enable
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
            Tunnel= Enabled
            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
            Tunnel= Disabled
            MLD Snooping= Disabled
            IGMP Snooping= Enabled

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 enabled

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

lan *NUMBER* **dvlan enabled**

lan dvlan disabled

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

lan *NUMBER* **dvlan disabled**

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

supplicant username *WORD*

Set the username for AP 802.1X supplicant

supplicant password *WORD*

Set the password for AP 802.1X supplicant

supplicant mac

Set the username and password to use AP MAC address for AP 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 the 802.1X authentication server for the AP, 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 the 802.1X accounting server for the AP, 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)#
```

preferred-master

To enable the Preferred Master and secondary Preferred Master AP settings, enter the following command:

preferred-master ap-mac <PREFERRED-MAC> [<PREFERRED-SECONDARY-MAC>]

Syntax Description

<PREFERRED-MAC>

Eneter the MAC address of the primary Preferred Master.

<PREFERRED-SECONDARY-MAC>

Eneter the MAC address of the secondary Preferred Master.

Defaults

None.

Example

```
ruckus(config-ap-policy)# preferred-master ap-mac d4:c1:9e:35:a9:40
The Preferred Master function has been updated.
ruckus(config-ap-policy)#
```

> **NOTE**
> **preferred-master** command is not supported in Dedicated Master mode.

no preferred-master

To disabled the Preferred Master and secondary Preferred Master AP settings, enter the following command:

no preferred-master <PREFERRED-MAC> [<PREFERRED-SECONDARY-MAC>]

Defaults

Disabled.

Example

```
ruckus(config-ap-policy)# no preferred-master
The Preferred Master function has been updated.
ruckus(config-ap-policy)#
```

master-focus-controller

To enable the Focus Controller feature to allow the Master AP to focus on controller functions and not serve as a Wi-Fi access point, enter the following command:

master-focus-controller

Defaults

Disabled.

Example

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

> **NOTE**
> **master-focus-controller** command is not supported in Dedicated Master mode.

no master-focus-controller

To disable the Focus Controller feature, enter the following command:

no master-focus-controller

Defaults

Disabled.

Example

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

Keep AP's setting

Example

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

> **NOTE**
> **ap-management-vlan** command is supported only in Dedicated Master mode.

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.

Example

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

> **NOTE**
> **ap-auto-approve** command is supported only in Dedicated Master mode.

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-unleashed-discovery

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

limited-unleashed-discovery master-addr<*PRIMARY-ADDR*>[<*SECONDARY-ADDR*>]|**master-ip**<*PRIMARY-IP*>[<*SECONDARY-IP*>]|**keep-ap-setting**

Syntax Description

limited-unleashed-discovery

Configure devices to connect to a specific Unleashed

master-addr

Enables only APs connect to the specified Master and sets the primary Master's IP address

master-ip

Enables only APs connect to the specified Master and sets the primary Master's IP address

keep-ap-setting

Keeps the AP's original primary/secondary Master's address settings and preferred primary Master settings

PRIMARY

Address of primary Unleashed

SECONDARY

Address of secondary Unleashed

Defaults

Disabled.

Example

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

no limited-unleashed-discovery

To disable limited Unleashed discovery, use the following command:

no limited-unleashed-discovery

Syntax Description

no limited-unleashed-discovery

Disable limited Unleashed discovery

Defaults

Disabled.

Example

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

show

To display the Preferred Master and secondary Preferred Master AP settings, enter the following command:

show

Example

```
ruckus(config-ap-policy)# show
  Automatically approve all join requests from APs= Enabled
  Limited Unleashed Discovery:
    Status= Disabled
  Management VLAN:
    Status= Keep AP's setting
  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)#
```

> **NOTE**
> You can create a maximum of 10 AP groups in non-Dedicated mode and 32 AP groups in Dedicated mode.

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)#
```

exit

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

abort

Exits the config-ap-group context without saving changes.

quit

Exits the config-ap-group context without saving changes.

show

To display current AP group configuration settings, use the following command from within the config-ap-group context:

show

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)#
exit
```

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

wlan add

To add a WLAN service in the AP group, use the following command:

wlan *add name* **wlan_name**

Syntax Description

MAC

The MAC address of the device

Defaults

None.

Example

```
ruckus(config)# ap-group apgrp_aaa
The AP group 'apgrp_aaa' has been created. To save the AP group, type 'end' or 'exit'.
ruckus(config-apgrp)#
ruckus(config-apgrp)#
ruckus(config-apgrp)#
ruckus (config-apgrp)# wlan
add del
ruckus(config-apgrp)# wlan add name wlan_a
ruckus(config-apgrp)#
ruckus(config-apgrp)# end
The AP group 'apgrp_aaa' has been updated.
Your changes have been saved.
ruckus(config)#
ruckus(config)#
ruckus(config)# show ap-group
Name= apgrp_aaa
 WLAN Service:
            Wlan= wlan_a
```

wlan del

To delete a WLAN service in the AP group, use the following command:

wlan *del name* **wlan_name**

Syntax Description

MAC

The MAC address of the device

Defaults

None.

Example

```
ruckus(config)# ap-group apgrp_aaa
The AP group 'apgrp_aaa' has been created. To save the AP group, type 'end' or 'exit'.
ruckus(config-apgrp)#
ruckus(config-apgrp)#
ruckus(config-apgrp)#
ruckus (config-apgrp)# wlan
add del
ruckus(config-apgrp)# wlan add name wlan_a
ruckus(config-apgrp)# wlan add name wlan_b
ruckus(config-apgrp)# wlan del name wlan_a
ruckus(config-apgrp)#
ruckus(config-apgrp)# end
The AP group 'apgrp_aaa' has been updated.
Your changes have been saved.
ruckus(config)#
ruckus(config)#
ruckus(config)# show ap-group
Name= apgrp_aaa
 WLAN Service:
          Wlan= wlan_b
```

member add

To add a member in the AP group, use the following command:

member *add mac* **MAC**

Syntax Description

MAC

> The MAC address of the device

Defaults

None.

Example

```
ruckus(config)# ap-group apgrp_aaa
The AP group 'apgrp_aaa' has been created. To save the AP group, type 'end' or 'exit'.
ruckus(config-apgrp)#
ruckus(config-apgrp)#
ruckus(config-apgrp)# member add mac 34:fa:9f:1d:0d:20
ruckus(config-apgrp)# member add mac c8:03:f5:31:66:20
ruckus(config-apgrp)#
ruckus(config-apgrp)# end
The AP group 'apgrp_aaa' has been updated.
Your changes have been saved.
ruckus(config)# show ap-group
Members:
          MAC= 34:fa:9f:1d:0d:20
          MAC= c8:03:f5:31:66:20
```

member mac move-to

To add a member in the AP group, use the following command:

member *mac* **MAC move-to** *system-default name*

member *mac* **MAC move-to** *name* **ap_group**

Syntax Description

MAC

The MAC address of the device

name

The name of the AP group

Defaults

None.

Example

```
ruckus(config)# ap-group apgrp_aaa
The AP group entry 'apgrp_aaa' has been loaded. To save the AP group, type 'end' or 'exit'.
ruckus(config-apgrp)# member
add mac
ruckus(config-apgrp)# member mac 34:fa:9f:1d:0d:20 move-to
system-default name
ruckus(config-apgrp)# member mac 34:fa:9f:1d:0d:20 move-to name apgrp_bbb
ruckus(config-apgrp)#
ruckus(config-apgrp)#
ruckus(config-apgrp)# end
The AP group 'apgrp_aaa' has been updated.
Your changes have been saved.
ruckus(config)#
ruckus(config)#
ruckus(config)# show ap-group
APGROUP:
Name= apgrp_aaa
Members:
          MAC= c8:03:f5:31:66:20

Name= apgrp_bbb
Members:
          MAC= 34:fa:9f:1d:0d:20
```

Configure Location Based Service Commands

Use the following commands to to create and configure location services for an AP group. Use the location-services command to enter the **config-location-services** context from within the **config** context.

location-services

To create and begin configuring location services for this AP group, use the following command:

location-services *WORD*

Syntax Description

help

Set the IP addressing mode

history

IPv4, IPv6 or dual

abort

Exits the config-location-services context without saving changes.

end

Saves changes, and then exits the config-location-services context.

exit

Saves changes, and then exits the config-location-services context.

quit

Exits the config-location-services context without saving changes.

fqdn *WORD*

Sets the location server FQDN.

port *PORT-NUM*

Sets the location server port.

password *WORD*

Sets the location server preshared key.

show

Displays configured location services for all venues.

Example

```
ruckus(config)# location-services locationservice1
The location venue 'locationservice1' has been created. To save it, type 'end' or 'exit'.
ruckus(config-location-services)# fqdn example1.ruckuswireless.com
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-location-services)# port 8883
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-location-services)# password password
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-location-services)# end
The location venue 'locationservice1' has been updated and saved.
Your changes have been saved.
ruckus(config)#
```

no location-services

To disable location-based service on this AP group, use the following command:

no location-services *WORD*

Example

```
ruckus(config)# no location-service locationservice1
The location venue 'locationservice1' has been deleted.
ruckus(config)#
```

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

mesh mode

Use the mesh mode command from within the config-apgrp context to configure the group'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-apgrp)# mesh mode auto
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-apgrp)#
```

no meshmode-override

To disable the override of the mesh mode settings for the AP group, use the following command:

no meshmode-override

Defaults

Disabled.

Example

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

maxhops

To set the maximum mesh hops for the AP (0-3), use the following command:

maxhops *<NUMBER>*

Example

```
ruckus(config-ap)# maxhops 3
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-ap)#
```

channelflyoff

The ChannelFly override setting allows APs to disable ChannelFly if the AP's uptime is higher than the specified value (in minutes). To enable the ChannelFly override feature for the AP group, use the following command:

Defaults

Disabled

30 minutes

Example

```
ruckus(config-apgrp)# channelflyoff 30
ruckus(config-apgrp)# show
APGROUP:
        ID:
            :
              Name= apgroup2
              Description=
              Channel Range:
                B/G/N= 1,2,3,4,5,6,7,8,9,10,11 (Disallowed= )
                A/N Indoor= 36,40,44,48,149,153,157,161 (Disallowed= )
                A/N Outdoor= 36,40,44,48,149,153,157,161 (Disallowed= )
              Radio 11bgn:
                Channelization= Auto
                Channel= Auto
                Tx. Power= Auto
                11N only Mode= Auto
                WLAN Group= Default
                Call Admission Control= OFF
                SpectraLink Compatibility= Disabled
              Radio 11an:
                Channelization= Auto
                Indoor Channel= Auto
                Outdoor Channel= Auto
                Tx. Power= Auto
                11N only Mode= Auto
                WLAN Group= Default
                Call Admission Control= OFF
                SpectraLink Compatibility= Disabled
              Network Setting:
                Protocol mode= Use Parent Setting
              Turn off channfly setting: enabled
                if AP's uptime is more than 30 minutes will turn off AP's ChannelFly
              Members:

ruckus(config-apgrp)#
```

no channelflyoff

To disable the ChannelFly off feature for the AP group, use the following command:

no channelflyoff

no channelflyoff-override

To disable the override of ChannelFly settings (use parent settings), use the following command:

no channelflyoff-override

Example

```
ruckus(config-apgrp)# no channelflyoff-override
ruckus(config-apgrp)# show
APGROUP:
        ID:
            :
              Name= apgroup2
              Description=
              Channel Range:
                B/G/N= 1,2,3,4,5,6,7,8,9,10,11 (Disallowed= )
                A/N Indoor= 36,40,44,48,149,153,157,161 (Disallowed= )
```

```
        A/N Outdoor= 36,40,44,48,149,153,157,161 (Disallowed= )
      Radio 11bgn:
        Channelization= Auto
        Channel= Auto
        Tx. Power= Auto
        11N only Mode= Auto
        WLAN Group= Default
        Call Admission Control= OFF
        SpectraLink Compatibility= Disabled
      Radio 11an:
        Channelization= Auto
        Indoor Channel= Auto
        Outdoor Channel= Auto
        Tx. Power= Auto
        11N only Mode= Auto
        WLAN Group= Default
        Call Admission Control= OFF
        SpectraLink Compatibility= Disabled
      Network Setting:
        Protocol mode= Use Parent Setting
      Turn off channfly setting: Use Parent Setting
      Members:

ruckus(config-apgrp)#
```

radio (AP Group)

Configures the 2.4, 5, and 6 GHz radio settings independently on an AP Group.

Syntax

radio { **2.4** | **5** | **6** } [**channelization** { **auto**] [**auto-channel-selection** { *four-channel* | *three-channel* }| *number* }] [**channel** { **auto** | *number* }] [**tx-power** { **auto** | **full** | **min** | *1-10* }] [**wlan-group** *group_name*] [**wlan-service** { *enable* | *disable* } [**admission-control** *value*] [**channel-range** *number-list*]

no radio { **2.4** | **5** | **6** } [**channelization-override**] [**channel-override**] [**tx-power-override**] [**channel-range-override**]

Command Default

The default radio setting values are:

Parameter	Value
channelization	Auto
channel	Auto
auto-channel-selection	Three-channel
tx-power	Auto
wlan-group	Default
wlan-service	Enabled
wlan-service-override	Disabled
tx-power	Auto
admission-control	Disabled
spectralink-compatibility	Disabled

Parameters

2.4

Configures the 2.4 GHz radio.

5

Configures the 5 GHz radio.

6

Configures the 6 GHz radio. This option is supported only in tri-band APs.

channelization { **auto** | *number* }

AP channel width. For the 2.4 GHz radio, valid values are auto, 20, or 40 MHz. For the 5 GHz radio, valid values are auto, 20, 40, and 80, 160 MHz. For the 6 GHz radio, valid values are auto, 20, 40, 80, 160, and 320 MHz.

channel { **auto** | *number* }

AP channel. Valid values are auto or a specific channel number. Valid values are from 1 through 233 for 20 MHz, or from 1 through 229 for 40 MHz, or from 1 through 221 for 80, 160, or 320 MHz channels.

auto-channel-selection { *four-channel* | *three-channel* }

AP auto channel selection. Valid values for the four-channel are 1, 5, 9, and 13, and for three-channel are 1, 6, and 11.

tx-power { **auto** | **full** | **min** | **num** *1-10* }

AP transmit power. Valid values are auto, full, min, or a specific dB value in the range of -1 through -10.

admission-control *value*

Call admission control airtime usage limit (as a precentage). Valid values are 10%, 20%, 30%, 40%, 50%, 60%, and 70%.

channel-range *number-list*

Channels allowed.

wlan-group *group_name*

WLAN group name.

wlan-service { **enable** | **disable** }

Enable WLAN service on this radio

wlan-service-override

Enable the override of the WLAN service settings for this radio.

spectralink-compatibility

Enable SpectraLink Compatibility settings on the radio (sets DTIM=2, minrate=5.5Mbps and enable RTS-CTS protection mode).

no channelization-override

Disables the override of the channelization settings.

no channel-override

Disables the override of the channels.

no tx-power-override

Disables the override of the radio transmit power.

no channel-range-override

Disables the override of the channel range.

Modes

AP Group configuration mode

Usage Guidelines

The *6 GHz* radio can be configured only on the tri-band APs.

The **no** form of the command removes the configured values for the radios, reverting to the default configuration settings.

Examples

The following example configures the 2.4 GHz radio settings on an AP Group.

```
ruckus# config
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 5 channel auto channelization auto wlan-group Default tx-power Num 1
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-apgrp)#
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
WLAN Group= Default
Radio 11an:
Channelization= Auto
Channel= Auto
Tx. Power= 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
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)#
```

History

Release version	Command history
200.16	This command was modified to include the 6 GHz radio setting.

QoS Commands (AP)

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.

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.

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.

port-setting

Configures the port setting for the specified AP model. Enters config-apgrp-port context. See port-setting on page 192 for more information.

status-leds

Configures the status LEDs for the specified AP model (enable, disable).

external-antenna

Configures external antenna settings. See external-antenna on page 191.

max-clients *NUMBER*

Sets the maximum clients 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)

cband-license

Enable or disable 5.8 GHz Channels License for the specified AP model.

lacp-status

Configure LACP status for the specified AP model.

power-mode

Sets the PoE mode for the specified AP model.

802.3af-txchain

Sets the 2.4GHz radio transmit chains in 802.3af PoE mode for the specified AP model.

Defaults

Status LEDs: Enabled

PoE Out: Disabled

Internal Heater: Disabled

C-band channels: Disabled

C-band license: Disabled

LACP status: Disabled

Power mode: Varies by AP model

Power Mode: Default

802.3af-txchain: Varies by AP model

Example

```
ruckus(config-apgrp)# model R610 status-leds enable
ruckus(config-apgrp)# end
The AP group 'System Default' has been updated.
Your changes have been saved.
ruckus(config)#
```

no model

To disable model-specific settings for all APs of a certain model within an AP group, 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., r500, r600, r700, r710, r720, r510, r610, t710, t710s, t300, t300e, t301n, t301s, h510, r310, c110, t610, t610s, t310d, h320, t310c, t310n, t310s, e510, r730, r320).

status-leds-override

    Disables the override of the status LEDs for the specified AP model.

radio-band-override

    Disables the override of the radio band 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.

cband-license-override

    Disables the override of the 5.8GHz Channels license for this specified ap model.

external-antenna-override

    Disables the override of external antenna settings for this specified ap model.

lacp-status-override

    Disables the override of the status LACP for this specified ap model.

power-mode-override

Disables the override of the PoE mode for this specified ap model.

802.3af-txchain-override

Disables the override of the 2.4GHz radio transmit chains in 802.3af PoE mode for this specified ap model.

Defaults

Status LEDs: Enabled

Internal Heater: Disabled

C-band channels: Disabled

C-band license: Disabled

LACP status: Disabled

Power mode: Varies by AP model

Power Mode: Default

802.3af-txchain: Varies by AP model

Example

```
ruckus(config-apgrp)# no model R610 status-leds-override
ruckus(config-apgrp)# end
The AP group 'apgroup2' has been updated.
Your changes have been saved.
ruckus(config)#
```

external-antenna

To configure the external antenna settings for all APs of the specified model within the AP group, use the following command:

external-antenna *<WORD>*

Syntax Description

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.

port-setting

To modify model-specific port settings for all APs of the specified model within the AP group, use the following command:

model<*WORD*>**port-setting**

Syntax Description

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* **rate-uplink** *NUMBER*

Sets the uplink rate limiting for the port (0-1000).

lan *NUMBER* **rate-downlink** *NUMBER*

Sets the downlink rate limiting for the port (0-1000).

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* **tunnel disabled**

Disables the AP port tunnel settings.

lan *NUMBER* **tunnel enabled**

Enables the AP port tunnel 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.

lan *NUMBER* **qos directed-mcast**

Enables the AP port Directed Multicast 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 lan *NUMBER* **qos directed-mcast**

Disables the AP port Directed Multicast 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 zf7372 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
           Tunnel= 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
           Tunnel= Disabled
           MLD Snooping= Disabled
           IGMP Snooping= Enabled

ruckus(config-apgrp-port)#
```

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 rate-uplink

To set rate limiting on a port, use the following command:

lan *NUMBER* **rate-uplink** *NUMBER*

> **NOTE**
> The **rate-uplink** command is supported only for H550/H350 or H320/H510 in Gateway model.

Syntax Description

lan

Configure a specific port

NUMBER

Configure this port

rate-uplink

Set the uplink rate limiting

NUMBER

Enter the rate limiting to {NUMBER} Mbps, valid range is from 0 to 1000.

Defaults

None.

Example

```
ruckus(config-apgrp-port)# lan 1 rate-uplink 100
ruckus(config-apgrp-port)# show
PORTS:
    LAN ID:
        1:
            Rate Uplink= 100
ruckus(config-apgrp-port)#
```

lan rate-downlink

To set rate limiting on a port, use the following command:

lan *NUMBER* **rate-downlink** *NUMBER*

> **NOTE**
> The **rate-downlink** command is supported only for H550/H350 or H320/H510 in Gateway model.

Syntax Description

lan

Configure a specific port

NUMBER

Configure this port

rate-downlink

Set the downlink rate limiting

NUMBER

Enter the rate limiting to {NUMBER} Mbps, valid range is from 0 to 1000.

Defaults

None.

Example

```
ruckus(config-apgrp-port)# lan 1 rate-downlink 300
ruckus(config-apgrp-port)# show
PORTS:
    LAN ID:
        1:
            Rate Uplink= 300
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**

lan qos directed-mcast

To enable Directed Multicast for the port, use the following command:

lan *NUMBER* **qos directed-mcast**

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 lan qos directed-mcast

To disable Directed Multicast on the port, use the following command:

no lan *NUMBER* **qos directed-mcast**

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

LLDP Commands

To enable, disable or configure the Link Layer Discovery Protocol (LLDP) commands for the AP group, use the following commands from within the **config-apgrp** context.

lldp

To enable, disable or configure the AP group's Link Layer Discover Protocol settings, use the following commands.

Syntax Description

lldp

Configure LLDP settings.

enable

Enable LLDP with current settings.

disable

Disable LLDP with current settings.

interval *NUMBER*

Set packet transmit interval in second(s).

holdtime *NUMBER*

Set amount of time receiving device should retain the information.

ifname eth *NUMBER*

Enter the AP port number.

mgmt enable

Enable LLDP management IP address of the AP.

mgmt disable

Disable LLDP management IP address of the AP.

Example

```
ruckus(config-apgrp)# lldp enable
ruckus(config-apgrp)#
```

no lldp

To allow ZoneDirector to modify AP's LLDP settings, use the following command:

no lldp keep-ap-settings

Syntax Description

no lldp keep-ap-settings

Example

```
ruckus(config-ap)# no lldp keep-ap-setting
ruckus(config-ap)#
```

lldp keep-ap-setting

To not let the controller modify the AP's LLDP settings, use the following command:

lldp keep-ap-setting

Example

```
ruckus(config-apgrp)# lldp keep-ap-setting
ruckus(config-apgrp)#
```

no lldp keep-ap-setting

To allow the controller to modify the AP's LLDP settings, use the following command:

no lldp keep-ap-setting

Example

```
ruckus(config-apgrp)# no lldp keep-ap-setting
ruckus(config-apgrp)#
```

power-mode

To set the PoE mode of the AP, use the following command:

model *WORD* **power-mode** *WORD*

Syntax Description

model *WORD*

Set the AP model.

power-mode

Set the AP's PoE power mode.

auto

Set the power mode to Auto.

802.3af

Set the power mode to 802.3af.

802.3at

Set the power mode to 802.3at.

Example

```
ruckus(config-apgrp)# model R710 power-mode auto
ruckus(config-apgrp)#
```

no power-mode-override

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

no model *WORD* **power-mode-override**

802.3af-txchain

To set the number of 2.4 GHz radio transmit chains in 802.3af power mode for the AP, use the following command:

model *WORD* **802.3af-txchain** *WORD*

Syntax Description

model *WORD*

Set the AP model.

802.3af-txchain

Set the number of 2.4 GHz radio chains.

1

Set the radio chains to 1.

2

Set the radio chains to 2.

4

Set the radio chains to 4.

Example

```
ruckus(config-apgrp)# model R710 802.3af-txchain 1
ruckus(config-apgrp)#
```

no 802.3af-txchain-override

To disable the override of the 2.4 GHz radio transmit chains in 802.3af PoE mode, use the following command:

no model *WORD* **802.3af-txchain-override**

Bonjour Fencing Commands

Use the following commands to deploy a fencing policy to an AP group.

bonjour-fencing

To enable or disable Bonjour fencing, or apply a fencing policy to an AP group, use the following command:

Syntax

bonjour-fencing { **enable** | **disable** | [**policy** *<NAME>*]

Command Default

Disabled.

Parameters

enable

Enables Bonjour fencing.

disable

Disables Bonjour fencing.

policy

Designates an existing fencing policy for the WLAN.

Examples

```
ruckus(config-apgrp)# bonjour-fencing enable
Please choose a policy before bonjour-fencing is enabled!
ruckus(config-apgrp)# bonjour-fencing disable
ruckus(config-apgrp)# bonjour-fencing policy fence1
This bonjour fencing policy does not exist
ruckus(config-apgrp)#
```

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.

acl

To create a new L2 ACL entry or update an existing entry, use the following command:

acl *WORD*

Syntax Description

acl

Create a new ACL

WORD

Assign this name to the new ACL

Defaults

None.

Example

```
ruckus(config)# l2acl l2acl1
The L2 ACL entry 'l2acl1' has been created.
ruckus(config-l2acl)#
```

no acl

To delete an L2 ACL, use the following command:

no acl *WORD*

Syntax Description

no acl

Delete an existing ACL

WORD

Delete this ACL

Defaults

None.

Example

```
ruckus(config)# no l2acl l2acl1
The L2 ACL 'l2acl1' has been deleted.
ruckus(config)#
```

abort

To exit the config-l2acl context without saving changes, use the following command:

abort

end

To save changes, and then exit the config-l2acl context, use the following command:

end

Example

```
ruckus(config-l2acl)# 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

Example

```
ruckus(config-l2acl)# 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

Example

```
ruckus(config-l2acl)# quit
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

Example

```
ruckus(config-l2acl)# show
L2/MAC ACL:
```

```
   ID:
     :
       Name= l2acl1
       Description=
       Restriction= Deny only the stations listed below
       Stations:
         MAC Address= 00:11:22:33:44:55

ruckus(config-l2acl)#
```

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)# l2acl l2acl1
The L2 ACL entry 'l2acl1' has been created.
ruckus(config-l2acl)# name L2-ACL-1
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-l2acl)#
```

description

To set the description of an L2 ACL entry, use the following command (multiple word text must be enclosed in quotation marks):

description *WORD*

Syntax Description

description *WORD*

Set the L2 ACL description.

Defaults

None.

Example

```
ruckus(config)# l2acl l2acl1
The L2 ACL entry 'l2acl1' has been created.
```

```
ruckus(config-l2acl)# description "L2 ACL 1"
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-l2acl)#
```

add-mac

To add a MAC address to the L2 ACL, use the following command:

add-mac *MAC* [**DESCRIPTION**]

Syntax Description

add mac

Add a MAC address to the ACL

MAC

Add this MAC address

DESCRIPTION

Add a description for this MAC address

Defaults

None.

Example

```
ruckus(config-l2acl)# 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)#
```

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-l2acl)# mode allow
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-l2acl)#
```

mode deny

To set the ACL mode to 'deny', use the following command:

mode deny

Syntax Description

mode deny

   Set the ACL mode to deny

Defaults

None.

Example

```
ruckus(config-l2acl)# mode deny
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-l2acl)#
```

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** 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)#
```

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

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

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

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

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

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 (multiple word text must be enclosed in quotes):

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'.
```

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)#
```

source address

To set the source address of a L3/L4/IP ACL rule, use the following command:

source address <IP-ADDR/WORD>

Example

```
ruckus(config-l3acl-rule)# source address 192.168.0.1/24
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-l3acl-rule)#
```

source port

To set the source port of a L3/L4/IP ACL rule, use the following command:

source port <NUMBER/WORD>

Example

```
ruckus(config-l3acl-rule)# source port 880
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-l3acl-rule)#
```

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.
```

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

exit

To save changes, and then exit the config-l3acl-rule context, use the following command:

exit

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 (multiple word text must be enclosed in quotes):

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

Example

```
ruckus(config-l3acl)# show
L3/L4/IP ACL:
  ID:
    :
      Name= l3acl1
      Description=
      Default Action if no rule is matched= Deny all by default
      Rules:
        1:
          Description=
          Type= Allow
          Destination Address= 192.168.1.22/24
          Destination Port= 53
          Protocol= Any
        2:
          Description=
          Type= Allow
          Destination Address= Any
          Destination Port= 67
          Protocol= Any

ruckus(config-l3acl)#
```

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)#
```

no prece

To delete a precedence policy entry, use the following command:

no prece *WORD*

end

To save changes, and then exit the config-prece context, use the following command:

end

Example

```
ruckus(config-prece)# end
The Precedence Policy entry has saved successfully.
Your changes have been saved.
ruckus(config)#
```

exit

To save changes, and then exit the config-prece context, use the following command:

exit

Example

```
ruckus(config-prece)# exit
The Precedence Policy entry has saved successfully.
Your changes have been saved.
ruckus(config)#
```

quit

To exit the config-prece context without saving changes, use the following command:

quit

Example

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

name

Sets the Precedence Policy entry name.

description

Sets the Precedence Policy entry description.

show

To display the precedence settings, use the show command from within the config-prece context.

show

Example

```
ruckus(config-prece)# show
Precedence Policy:
  ID:
    2:
      Name= precedence1
      Description=
      Rules:
        1:
          Description=
          Attribute = vlan
          Order = AAA,Device Policy,WLAN
        2:
          Description=
          Attribute = rate-limit
          Order = AAA,Device Policy,WLAN

ruckus(config-prece)#
```

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-prece)#
ruckus(config-prece)# end
The Precedence Policy entry has saved successfully.
Your changes have been saved.
```

description

To set the Precedence Policy rule description, use the following command:

description

Example

```
ruckus(config-prece-rule)# description "Default precedence policy"
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-prece-rule)#
```

order

To set the order of the precedence policy, use the following command from within the config-prece-rule context.

order <WORD>

Syntax Description

<WORD>: Enter the order of Precedence Policy (for examle, "AAA" "Device Policy" "WLAN").

Example

```
ruckus(config-prece-rule)# order "AAA" "Device Policy" "WLAN"
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-prece-rule)#
```

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)#
```

no dvcpcy

To delete a device policy, use the following command:

no dvcpcy *WORD*

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.

dvctype *WORD*

Sets the device type of a Device Policy rule.

osvendor *WORD*

Sets the os vendor 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.

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)#
```

Configure Application Policy Commands

Use the following commands to create or modify application policies.

app-policy

To create a new application policy or modify an existing policy, use the following command:

app-policy *WORD*

Syntax Description

app-policy: Creates a new Application Policy entry or modifies an existing entry.

<WORD>: Enter a name for the application policy.

Example

```
ruckus(config)# app-policy policy1
The Application Policy entry 'policy1' has been created.
ruckus(config-app-policy)#
```

no app-policy

To delete an Application Policy entry, use the following command:

no app-policy *WORD*

Example

```
ruckus(config)# no app-policy policy1
The Application Policy 'policy1' has been deleted.
ruckus(config)#
```

description

To set the description for the policy, use the following command:

description *<WORD>*

Example

```
ruckus(config-app-policy)# description "Block Facebook"
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-app-policy)#
```

show

To display the application policy settings, use the show command from within the config-app-policy context.

show

Example

```
ruckus(config-app-policy)# show
Application Policy:
  ID:
    :
      Name= policy1
      Description=
      Rules:
        1:
          Rule Type= Denial Rules
          Application Type= System Defined
          Category= Social networks
          Application= Facebook

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

Configure Application Policy Rules

Use the following commands to configure application policy rules.

rule

Creates a new application policy rule or modifies an existing entry. Enters the *config-app-policy-rule* context.

rule *NUMBER*

Syntax Description

rule: Create or modify an application policy rule.

<NUMBER>: Enter a rule ID.

Example

```
ruckus(config-app-policy)# rule 1
ruckus(config-app-policy-rule)#
```

no rule

To delete a rule, use the following command:

no rule *NUMBER*

rule-type

To set the application policy rule type, use the following command:

rule-type*<WORD>*

Syntax Description

rule-type: Sets Application Policy rule type.

<WORD>: Enter rule type(Denial Rules | QoS | Rate Limiting).

Example

```
ruckus(config-app-policy-rule)# rule-type Denial Rules
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-app-denial-rule)#
```

application-type

To set the application type, use the following command:

application-type*<WORD>*

Syntax Description

application-type: Sets Application Policy rule application type.

<WORD>: Enter application type ("System Defined" or "Port base User Defined Application" or "IP base User Defined Application" or "Application name").

Example

```
ruckus(config-app-denial-rule)# application-type System Defined
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-app-denial-rule)#
```

category

To set the application category, use the following command:

category*<WORD>*

Syntax Description

category: Sets Application Policy rule application category.

<LIST>: Enter application name: [Instant messengers|Peer-to-peer networks|File sharing services and tools|Media streaming services|Email messaging services|VoIP services|Database tools|Online games|Management tools and protocols|Remote access terminals|Tunneling and proxy services|Investment platforms|Web services|Security update tools|Web instant messengers|Business tools|Network protocols (18)|Network protocols (19)|Network protocols (20)|Private protocols|Social networks]

Example

```
ruckus(config-app-denial-rule)# category Social networks
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-app-denial-rule)#
```

application

To set the application, use the following command:

application*<WORD>*

Syntax Description

category: Sets Application Policy rule application name.

<LIST>: |Classmates|Yik Yak|Facebook|Flickr|Hi5|LinkedIn|Livejournal|Twitter|Plurk|MySpace|Khan Academy|Pinterest|Tumblr|MeetMe|VKontakte|Odnoklassniki|Niwota|Tagged|PerfSpo t|Me2day|Mekusharim|Draugiem|Badoo|Meetup|Foursquare|Ning|i-Part/iPair|Dudu|M ig33|Hatena|eHarmony|Fotolog |Tencent QQ|Pixnet|Nk.Pl|Twoo|Plaxo|Cyworld|Jivesoftware|WordPress|FMyLife|Dcinside|Cl ass Chinaren|Bai Sohu|Yammer|Douban|Gamer|Xuite|ChatMe|Clien.net|AdultFriendFinder|Fling.com|D elicious|Mei.fm|Streetlife|Daum-blog|Naver-blog|Panoramio|Blogger|FC2|Yahoo Blog|Friendster|Ameba|Bebo social network|Kaixin|Orkut|Aol-Answers|CoolTalk social network|RenRen.com|TweetDeck|Hootsuite|Xing|Lokalisten|meinVZ/studiVZ|Viadeo| Tuenti|Hyves|Mixi.jp|Yahoo-mbga.jp|GREE|Netlog|2ch|LoveTheseCurves|Weibo|Goog le+|Skyrock|51.com|Jackd|Touch|Skout|Instagram|Jiayuan|Zoosk|DatingDNA|500px| iAround|pairs|Path|WeHeartIt|Fancy|Vine|SnappyTV|Miliao|After School|Weico|

Example

```
ruckus(config-app-denial-rule)# application Facebook
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-app-denial-rule)#
```

Configuring User-Defined Applications

Use the following commands to configure user-defined IP-based applications. Once created, user-defined applications can be controlled using the application policy commands.

user-app-ip

To configure IP-based user-defined application settings, and enter the config-user-app-ip context, use the following command:

user-app-ip

Example

```
ruckus(config)#  user-app-ip Application1
The User Defined Application entry Application1 has been created.
ruckus(config-user-app-ip)#
```

no user-app-ip

To delete a user-defined application entry, use the following command:

no user-app-ip*WORD*

Example

```
ruckus(config)# no user-app-ip Application1
The policy 'Application1' has been removed .
ruckus(config)#
```

abort

Exits the config-user-app-ip context without saving changes.

end

Saves changes, and then exits the config-user-app-ip context.

exit

Saves changes, and then exits the config-user-app-ip context.

destination-IP

To set the destination address of a user-defined application entry, use the following command:

destination-IP *IP-ADDR*

Example

```
ruckus(config-user-app-ip)# destination-IP 192.168.40.3
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-user-app-ip)#
```

netmask

To set the netmask of a user-defined application, use the following command:

netmask *IP-ADDR*

Example

```
ruckus(config-user-app-ip)# netmask 255.255.255.0
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-user-app-ip)#
```

destination-port

To set the destination port of a user-defined Application, use the following command:

destination-port *NUMBER*

Example

```
ruckus(config-user-app-ip)# destination-port 883
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-user-app-ip)#
```

protocol

To set the protocol of a user-defined application, use the following command:

protocol *WORD*

Example

```
ruckus(config-user-app-ip)# protocol tcp
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-user-app-ip)#
```

application-name

To set the name the application, use the following command:

application *WORD*

Example

```
ruckus(config-user-app-ip)# application-name Blocked-Application-1
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-user-app-ip)#
```

Configuring User-Defined Applications Based on Port Mapping

Use the following commands to configure user-defined applications based on port mapping. Once configured, these user-defined applications can be controlled using the application policy commands.

user-app-port

Configures port-based user-defined application settings. Enters config-user-app-port context.

Example

```
ruckus(config)# user-app-port Application2
The Application Port Mapping entry Application2 has been created.
ruckus(config-user-app-port)#
```

no user-app-port

To delete a port-based user-defined application, use the following command:

no user-app-port *WORD*

Example

```
ruckus(config)# no user-app-port userapp1
The policy 'userapp1' has been removed .
ruckus(config)#
```

abort

Exits the config-user-app-port context without saving changes.

end

Saves changes, and then exits the config-user-app-port context.

exit

Saves changes, and then exits the config-user-app-port context.

port

To set the Port of the port-based application, use the following command:

port *NUMBER*

Example

```
ruckus(config-user-app-port)# port 443
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-user-app-port)#
```

protocol

To set the Protocol for the port-based user-defined Application, use the following command:

protocol *WORD*

Example

```
ruckus(config-user-app-port)# protocol tcp
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-user-app-port)#
```

application-name

To set the application name, use the following command:

application-name*<WORD>*

Example

```
ruckus(config-user-app-port)# application-name Application2
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-user-app-port)#
```

Configure Wi-Fi Calling Settings

Use the following commands to configure Wi-Fi calling settings.

wificalling

To configure Wi-Fi Calling with the specified profile name, use the following command:

wificalling enable profile *<WORD>*

Defaults

None

Example

```
ruckus(config)# wificalling profile1
The WIFI Calling "profile1" has been created.
ruckus(config-wifi-calling)#
```

no wificalling

To delete a WiFi Calling profile, use the following command:

no wificalling <WORD>

Defaults

None

Example

```
ruckus(config)# no wificalling profile1
The WIFI Calling Policy 'profile1' has been deleted.
ruckus(config)#
```

description

To set the Wi-Fi Calling policy entry description, use the following command:

description *<WORD>*

Example

```
ruckus(config-wifi-calling)# description "T-Mobile Wi-Fi Calling Profile"
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wifi-calling)#
```

no description

To remove the Wi-Fi Calling policy entry description, use the following command:

no description

Example

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

priority

To set the Wi-Fi Calling profile's priority level, use the following command:

priority [*voice* | *video* | *best-effort* | *background*]

Example

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

epdg domain

To set the Wi-Fi Calling EPDG domain name and IP address, use the following command:

epdg domain *<WORD>* ipv4 *<WORD>*

A maximum of five domain and IP address pairs can be configured.

Example

```
ruckus(config-wifi-calling)# epdg domain TMobile ipv4 192.168.9.99
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wifi-calling)#
```

no epdg domain

To delete the Wi-Fi Calling policy EPDG entry, use the following command:

no epdg domain *<WORD>* ipv4 *<WORD>*

Example

```
ruckus(config-wifi-calling)# no epdg domain tmobile ipv4 192.168.33.99
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wifi-calling)#
```

show

To display the current Wi-Fi Calling policy entry information, use the following command:

show

Example

```
ruckus(config-wifi-calling)# show
    :
      WIFI Calling Carrier Name: profile1
      WIFI Calling Priority: 1
          WIFI Calling Domains: tmobile
          WIFI Calling IP address:192.168.33.99
ruckus(config-wifi-calling)#
```

Configure URL Filtering Settings

Use the following commands to configure URL Filtering settings.

url-filtering

To configure a URL Filtering Profile and enter the *config-url-filtering* context, use the following command:

url-filteringNAME

Example

```
ruckus(config)# url-filtering filter1
The Url Filtering "filter1" has been created.
ruckus(config-url-filtering)#
  help                  Shows available commands.
  history               Shows a list of previously run commands.
  abort                 Exits the config-url-filtering context without saving changes.
  end                   Saves changes, and then exits the config-url-filtering-xxx context.
  exit                  Saves changes, and then exits the config-url-filtering-xxx context.
  show                  Displays the current Url Filtering settings.
  no                    Contains commands that can be executed from within the context.
  description <WORD>    Sets the Policy entry description.
  filtering-level <WORD>
                        Selects a filtering categories level.
  blocked-category <list>
                        Selects the blocked categories only for "CUSTOM" (for example: Abortion,
                        Abused Drugs, Auctions).
  create-blocklist <domain>
                        Creates a new Blocklist.
  delete-blocklist <domain>
                        Deletes a exist Blocklist.
  create-allowlist <domain>
                        Creates a new Allowlist.
  delete-allowlist <domain>
                        Deletes a exist Allowlist.
  google-safe-search    Enables Google Safe Search.
  google-ip <IP-ADDR>   Configures Google Safe Search Virtual IP(216.239.38.120).
  youtube-safe-search   Enables YouTube Safe Search.
  youtube-ip <IP-ADDR>
                        Configures YouTube Safe Search Virtual IP(216.239.38.120).
  bing-safe-search      Enables Bing Safe Search.
  bing-ip <IP-ADDR>     Configures Bing Safe Search Virtual IP(204.79.197.220).
ruckus(config-url-filtering)#
```

no url-filtering

To delete a URL Filtering Profile, use the following command:

no url-filteringNAME

Example

```
ruckus(config)# no url-filtering filter1
The policy 'filter1' has been removed .
ruckus(config)#
```

description

To set the URL Filtering policy entry description, use the following command:

description *<WORD>*

Example

```
ruckus(config-url-filtering)# description "Filter 1"
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-url-filtering)#
```

filtering-level

To select a filtering level category, use the following command:

filtering-level *NO_ADULT | CLEAN_AND_SAFE | CHILD_AND_STUDENT_FRIENDLY | STRICT | CUSTOM*

Example

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

blocked-category

To select a blocked category (only for "CUSTOM" for example: Abortion, Abused Drugs, Auctions), use the following command:

blocked-category *Abortion, Abused Drugs, Adult and Pornography, Alcohol and Tobacco, Auctions, Bot Nets, Business and Economy, Cheating, Computer and Internet Info, Computer and Internet Security, Confirmed SPAM Sources, Content Delivery Networks, Cult and Occult, Dating, Dead Sites, Dynamic Comment, Educational Institutions, Entertainment and Arts, Fashion and Beauty, Financial Services, Food and Dining, Gambling, Games, Government, Gross, Hacking, Hate and Racism, Health and Medicine, Home and Garden, Hunting and Fishing, Illegal, Image and Video Search, Internet Communications, Internet Portals, Job Search, Keyloggers and Monitoring, Kids, Legal, Local Information, Malware Sites, Marijuana, Military, Motor Vehicles, Music, News and Media, Nudity, Online Greeting cards, Open HTTP Proxies, Parked Domains, Pay to Surf, Peer to Peer, Personal Storage, Personal sites and Blogs, Philosophy and Political Advocacy, Phishing and Other Frauds, Private IP Addresses, Proxy Avoidance and Anonymizers, Questionable, Real Estate, Recreation and Hobbies, Reference and Research, Religion, SPAM URLs, Search Engines, Sex Education, Shareware and Freeware, Shopping, Social Networking, Society, Sports, Spyware and Adware, Stock and Advice Tools, Streaming Media, Swimsuits & Intimate Apparel, Training and Tools, Translation, Travel, Unconfirmed SPAM Sources, Violence, Weapons, Web Advertisements, Web Hosting, Web based Email*

Example

```
ruckus(config-url-filtering)# blocked-category Violence
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-url-filtering)#
```

create-blocklist

To create a new domain blocklist, use the following command:

create-blocklist *<domain>*

Example

```
ruckus(config-url-filtering)# create-blocklist facebook.com
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-url-filtering)#
```

delete-blocklist

To delete a domain blocklist, use the following command:

delete-blocklist<*domain*>

Example

```
ruckus(config-url-filtering)# delete-blocklist facebook.com
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-url-filtering)#
```

create-allowlist

To create a domain allowlist, use the following command:

create-allowlist<*domain*>

Example

```
ruckus(config-url-filtering)# create-allowlist ruckuswireless.com
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-url-filtering)#
```

delete-allowlist

To delete a domain allowlist, use the following command:

delete-allowlist<*domain*>

Example

```
ruckus(config-url-filtering)# delete-allowlist ruckuswireless.com
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-url-filtering)#
```

google-safe-search

To enable Google Safe Search, use the following command:

google-safe-search

Example

```
ruckus(config-url-filtering)# google-safe-search
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-url-filtering)#
```

no google-safe-search

To disable Google Safe Search, use the following command:

no google-safe-search

Example

```
ruckus(config-url-filtering)# no google-safe-search
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-url-filtering)#
```

google-ip

To configure Google Safe Search Virtual IP (default: 216.239.38.120), use the following command:

google-ip*IP Address*

Defaults

216.239.38.120

google-ip*IP Address*

Example

```
ruckus(config-url-filtering)# google-ip 216.239.38.120
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-url-filtering)#
```

youtube-safe-search

To enable Youtube Safe Search, use the following command:

youtube-safe-search

Example

```
ruckus(config-url-filtering)# youtube-safe-search
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-url-filtering)#
```

no youtube-safe-search

To disable Youtube Safe Search, use the following command:

no youtube-safe-search

Example

```
ruckus(config-url-filtering)# no youtube-safe-search
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-url-filtering)#
```

youtube-ip

To configure the YouTube Safe Search Virtual IP (default: 216.239.38.120), use the following command:

youtube-ip *IP-ADDR*

Defaults

216.239.38.120

Example

```
ruckus(config-url-filtering)# youtube-ip 216.239.38.120
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-url-filtering)#
```

bing-safe-search

To enable Bing Safe Search, use the following command:

bing-safe-search

Example

```
ruckus(config-url-filtering)# bing-safe-search
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-url-filtering)#
```

no bing-safe-search

To disable Bing Safe Search, use the following command:

no bing-safe-search

Example

```
ruckus(config-url-filtering)# no bing-safe-search
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-url-filtering)#
```

bing-ip

To configure the Bing Safe Search Virtual IP (default: 204.79.197.220), use the following command:

bing-ip *IP-ADDR*

Defaults

204.79.197.220

Example

```
ruckus(config-url-filtering)# bing-ip 204.79.197.220
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-url-filtering)#
```

show

To display the current URL Filtering settings, use the following command:

show

Example

```
ruckus(config-url-filtering)# show
    :
    Url Name: filter1
    Filter Type: CUSTOM
    Number of Blocked Categories: 1
    Blocked Categories:
            Violence
    Blocklist-Domains:
            cisco.com
            facebook.com
    Allowlist-Domains:
            ruckuswireless.com
    Google Safe Search: Disabled
    YouTube Safe Search VIP: 216.239.38.120
    Bing Safe Search VIP: 204.79.197.220
ruckus(config-url-filtering)#
```

Configure Allowlist Commands

Use the allowlist command to create a new client isolation allowlist or modify an existing allowlist, and enter the **config-allowlist** context.

allowlist

To create a new allow list entry or modify an existing entry, use the following command:

allowlist *WORD*

no allowlist

To delete a allowlist entry, use the following command:

no allowlist *WORD*

name

To set the Allow List entry name, use the following command:

name *WORD*

description

To set the description of the allowlist entry, use the following command:

description *WORD*

auto_discover

To enable or disable auto discover state of the client isolation allowlist, use the following command:

auto_discover *enable | disable*

Configuring Allowlist Rules

Use the rule command from within the config-allowlist context to create a new rule or modify an existing rule, and enter the **config-allowlist-rule** context.

rule

To create a new allowlist rule or modify an existing rule, use the following command:

rule *NUMBER*

no rule

To delete a allowlist rule, use the following command:

no rule *NUMBER*

description

To set the Allow List rule description, use the following command:

description *WORD*

mac

To set the MAC address, use the following command (format: XX:XX:XX:XX:XX:XX):

mac *MAC*

ip

To set the IP address, use the following command (format: 172.18.110.12).

ip *IP*

Configure Band Balancing Commands

Client Band Balancing attempts to balance the number of clients across AP radios, allowing configurable thresholds for ratio of clients on the 2.4 vs. 5 GHz radio bands. Use the band-balancing commands to configure the controller's band balancing settings. To run these commands, you must first enter the **config-band-balancing** context.

band-balancing

To enable load-balancing and enter the config-band-balancing context, use the following command:

band-balancing

abort

Exits the band balancing context without saving changes.

end

Saves changes, and then exits the band balancing context.

exit

Saves changes, and then exits the band balancing context.

quit

Exits the band balancing context without saving changes.

enable

To enable band balancing, use the following command:

enable

Example

```
ruckus(config-band-balancing)# enable
The band balancing settings have been updated.
ruckus(config-band-balancing)#
```

disable

To disable band balancing, use the following command:

disable

Example

```
ruckus(config-band-balancing)# disable
The band balancing settings have been updated.
ruckus(config-band-balancing)#
```

Proactive

To enable or disable Proactive Band Balancing, use the following command:

Proactive <NUMBER>

Syntax

<NUMBER>: 0 for disable, 1 for enable

Example

```
ruckus(config-band-balancing)# proactive 0
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-band-balancing)#
```

percent-2.4G <NUMBER>

To configure the percentage of clients on the 2.4 GHz band, use the following command:

percent-2.4G <NUMBER>

Defaults

25

Example

```
ruckus(config-band-balancing)# percent-2.4G 25
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-band-balancing)#
```

show

Displays information about Band balancing.

Example

```
ruckus(config-band-balancing)# show
Band Balancing:
  Enable= 1
  Percent of clients on 2.4G band: 25%
  Proactive Status= 1

ruckus(config-band-balancing)#
```

Configure Load Balancing Commands

Client Load Balancing attempts to balance the number of clients across APs, per radio band. 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)#
```

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: 50

Wifi1: 43

Example

```
ruckus(config-load-balancing)# enable wifi0
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-load-balancing)# adj-threshold wifi0 25
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-load-balancing)# show
Load Balancing:
  Radio 0:
      Status= Enabled
      AdjacentThreshold= 25
      WeakBypass= 33
      StrongBypass= 55
      ActivationThreshold= 10
      NewTrigger= 3
      Headroom= 3
```

```
  Radio 1:
      Status= Disabled
      AdjacentThreshold= 43
      WeakBypass= 35
      StrongBypass= 55
      ActivationThreshold= 10
      NewTrigger= 3
      Headroom= 3


ruckus(config-load-balancing)#
```

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

wifi0: 33

wifi1: 35

Example

```
ruckus(config-load-balancing)# weak-bypass wifi0 33
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-load-balancing)#
```

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

55

Example

```
ruckus(config-load-balancing)# strong-bypass wifi0 55
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-load-balancing)#
```

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).

Defaults

10

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).

Defaults

> 3

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).

Defaults

> 3

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)#
```

disable wifi0

Disable wifi0 load balancing.

disable wifi1

Disable wifi1 load balancing.

enable wifi0

Enable wifi0 load balancing.

enable wifi1

Enable wifi1 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:
  Radio 0:
      Status= Enabled
      AdjacentThreshold= 50
      WeakBypass= 33
      StrongBypass= 55
      ActivationThreshold= 10
      NewTrigger= 3
      Headroom= 3

  Radio 1:
      Status= Disabled
      AdjacentThreshold= 43
      WeakBypass= 35
      StrongBypass= 55
      ActivationThreshold= 10
      NewTrigger= 3
      Headroom= 3


ruckus(config-load-balancing)#
```

Configure STP Commands

Both Ethernet ports are one logical interface. They are designed to provide high availability connections to separate switches and do not provide dual-port ISL channel bonding. Switches should use STP to block one path. The default is "no stp".

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 {arguments}*

Syntax Description

dot11-country-code

Configure the controller's country code setting

COUNTRY-CODE

Set the country code to this value

channel-mode

Contains commands that can be executed from within the context

allow-indoor

Allows ZoneFlex Outdoor APs to use channels regulated as indoor use-only

not-allow-indoor

Disallows ZoneFlex Outdoor APs to use channels regulated as indoor use-only

channel-optimization

Set channel optimization type (compatibility, interoperability, performance)

Defaults

None.

Example

To set the country code to US, enter the following command:

```
ruckus# configruckus(config)# system
ruckus(config-sys)# dot11-country-code US
The country code settings have been updated.
ruckus(config-sys)#
```

internet-check

To configure the internet-check feature, use the following command:

Syntax

internet-check < **COMPANY** >

Command Default

Enabled.

Examples

```
ruckus(config-sys)# internet-check all
The internet check settings have been updated.
ruckus(config-sys)# show internet-check
Internet Check:
Company = apple, Enable = 1

Internet Check:
Company = microsoft, Enable = 1

Internet Check:
Company = ruckus, Enable = 1

ruckus(config-sys)#
```

no internet-check

To disable the internet-check feature, use the following command:

Syntax

no internet-check< **COMPANY** >

Command Default

Enabled.

Examples

```
ruckus(config-sys)# no internet-check apple
The internet check settings have been updated.
ruckus(config-sys)# show internet-check
Internet Check:
Company = apple, Enable = 0

Internet Check:
Company = microsoft, Enable = 1

Internet Check:
Company = ruckus, Enable = 1

ruckus(config-sys)#
```

show internet-check

To display the current internet-check settings, use the following command:

Syntax

show internet-check

Command Default

None.

Examples

```
ruckus(config-sys)# show internet-check
Internet Check:
Company = apple, Enable = 1

Internet Check:
Company = microsoft, Enable = 1

Internet Check:
Company = ruckus, Enable = 1

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

192.168.0.1

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

IP address: 192.168.0.2

Subnet mask: 255.255.255.0

Example

```
ruckus# config
ruckus(config)# system
ruckus(config-sys)# interface
ruckus(config-sys-if)# ip addr 192.168.0.2 255.255.255.0
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)#
```

vlan

If Unleashed is on a tagged Access VLAN, to set the VLAN ID, use the following

command:

Syntax Description

vlan *NUMBER*

Enter the VLAN ID

Example

```
ruckus(config-sys-if)# vlan
  <NUMBER>             Enter the VLAN ID.

ruckus(config-sys-if)# show

Management VLAN:
  VLAN ID= 1
```

no ip

To disable IPv4 addressing, use the following command:

no ip

system-timezone

To configure time zone settings, use the following command:

system-timezone *<TIMEZONE>*

Defaults

GMT+0

Example

```
ruckus(config-sys)# system-timezone GMT+8
The timezone settings have been updated.
ruckus(config-sys)#
```

userdefined-timezone

To configure user-defined time zone, use the following command:

userdefined-timezone *<TIMEZONE>*

Defaults

None

Example

```
ruckus(config-sys)# userdefined-timezone GMT+8:30
The timezone settings have been updated.
ruckus(config-sys)#
```

system-dst

To configure system Daylight Savings Time settings, use the following command:

system-dst [enable | disable]

Defaults

Disabled

Example

```
ruckus(config-sys)# system-dst enable
The timezone settings have been updated.
ruckus(config-sys)#
```

no system-dst

To disable the system Daylight Savings Time settings, use the following command:

no system-dst

Defaults

Disabled

Example

```
ruckus(config-sys)# no system-dst
The timezone settings have been updated.
ruckus(config-sys)#
```

userdefined-dst

To configure user-defined Daylight Savings Time settings, use the following command:

userdefined-dst <DST>

Defaults

Disabled

Example

```
ruckus(config-sys)# userdefined-dst M1.1.0/00,M1.2.0/00
The timezone settings have been updated.
ruckus(config-sys)#
```

no userdefined-dst

To delete the user-defined Daylight Savings Time settings, use the following command:

no userdefined-dst

Defaults

Disabled

Example

```
ruckus(config-sys)# no userdefined-dst
The timezone settings have been updated.
ruckus(config-sys)#
```

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.

mgmt-if

To enable the management interface, use the following command:

mgmt-if

Defaults

Disabled.

Example

```
ruckus(config-sys)# mgmt-if
ruckus(config-sys-mgmt-if)#
  help                 Shows available commands.
  history              Shows a list of previously run commands.
  abort                Exits the config-sys-mgmt-if context without saving changes.
  end                  Saves changes, and then exits config-sys-mgmt-if context.
  exit                 Saves changes, and then exits config-sys-mgmt-if context.
  quit                 Exits the config-sys-mgmt-if context without saving changes.
  ip                   Contains commands that can be executed from within the context.
  show                 Displays current management interface settings.
ruckus(config-sys-mgmt-if)#
```

ip addr

To configure the IP address of the management interface, use the following command:

ip addr *IP-ADDR NET-MASK*

Syntax Description

IP-ADDR

Enter the IP address.

NET-MASK

Set the Netmask for the address.

Defaults

None.

Example

```
ruckus(config-sys-mgmt-if)# ip addr 192.168.40.4 255.255.255.0
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-sys-mgmt-if)#
```

vlan

To enable the management VLAN and set the VLAN ID, use the following command:

vlan *NUMBER*

Syntax Description

vlan *NUMBER*

Enter the VLAN ID

Example

```
ruckus(config-sys-mgmt-if)# vlan
  <NUMBER>              Enter the VLAN ID.

ruckus(config-sys-mgmt-if)# show

VLAN= 40
```

no mgmt-if

To disable the management interface, use the following command:

no mgmt-if

Defaults

Disabled.

Example

```
ruckus(config-sys)# no mgmt-if
The management interface has been updated.
ruckus(config-sys)#
```

Unleashed-Multi-Site-Manager

To configure UMM settings, use the following command:

Unleashed-Multi-Site-ManagerIP-ADDR DOMAIN-NAME interval <NUMBER>

Syntax Description

interval

   Configure UMM interval (1~60 minutes).

IP-ADDR

   Configure UMM IP address.

DOMAIN-NAME

   Configure UMM domain name.

Example

```
ruckus(config-sys)# Unleashed-Multi-Site-Manager www.ruckuswireless.com interval 15
The Unleashed Multi-Site Manager settings have been updated.
ruckus(config-sys)#
```

no Unleashed-Multi-Site-Manager

To disable UMM settings, use the following command:

no Unleashed-Multi-Site-Manager

Example

```
ruckus(config-sys)# no Unleashed-Multi-Site-Manager
Unleashed Multi-Site Manager has been disabled.
ruckus(config-sys)#
```

Unleashed-Multi-Site-Manager-Force

To configure Force UMM settings, use the following command:

Unleashed-Multi-Site-Manager-ForceIP-ADDR / DOMAIN-NAME interval <NUMBER>

Syntax Description

interval

Configure UMM interval (1~60 minutes).

IP-ADDR

Configure UMM IP address.

DOMAIN-NAME

Configure UMM IP address domain name.

Example

```
ruckus(config-sys)# Unleashed-Multi-Site-Manager-Force www.ruckuswireless.com interval 60
The Unleashed Multi-Site Manager settings have been updated.
ruckus(config-sys)#
```

no Unleashed-Multi-Site-Manager-Force

To disable Force UMM settings, use the following command:

no Unleashed-Multi-Site-Manager-Force

Example

```
ruckus(config-sys)# no Unleashed-Multi-Site-Manager-Force
Unleashed Multi-Site Manager has been disabled.
ruckus(config-sys)#
```

northbound

To enable northbound portal interface and set the northbound portal interface password, use the following command:

Syntax

northbound password [*WORD*]

Parameters

password

Set the northbound portal interface password

Examples

```
ruckus(config-sys)# northbound password password1234
The northbound portal interface settings have been updated.
ruckus(config-sys)#
```

no northbound

To disable northbound portal authentication, use the following command:

Syntax

no northbound

Command Default

Disabled.

Examples

```
ruckus(config-sys)# no northbound
Northbound portal interface has been disabled.
ruckus(config-sys)#
```

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.
```

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.
```

dedicated-master

To enable Dedicated Master, use the following command:

dedicated-master

Syntax Description

dedicated-master

Enables Dedicated Master mode.

Defaults

Disabled

Example

```
ruckus(config-sys)# dedicated-master
The System dedicated master will be enabled, the system will be rebooted, are you sure(y/n):y
ruckus(config-sys)# show

……
Dedicated Master:
  Status= Enabled
```

NOTE

Dedicated Master mode is supported only on R750 AP and R850 AP.

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

Syntax Description

smart-redundancy

    Configures smart redundancy settings.

help

    Shows available commands.

history

    Shows a list of previously run commands.

abort

    Exits the smart redundancy context without saving changes.

end

    Saves changes, and then exits the smart redundancy context.

exit

    Saves changes, and then exits the smart redundancy context.

quit

    Exits the smart redundancy context without saving changes

peer-addr *IP-ADDR*

    Sets the peer's IP/IPv6 address.

secret *WORD*

    Sets the shared secret to the specified secret.

show

    Displays information about smart redundancy.

Example

```
ruckus# config
ruckus(config)# system
ruckus(config-sys)# smart-redundancy
ruckus(config-sys-smart-redundancy)# show
Smart Redundancy:
  Status= Enabled
  Local Connect Status= Active
  Peer IP Address     = 10.223.55.91
  Peer Connect Status = Standby
  Shared Secret=
ruckus(config-sys-smart-redundancy)#
```

no smart-redundancy

Disables the smart redundancy settings.

Example

```
ruckus(config-sys)# no smart-redundancy
The smart redundancy settings have been updated.
ruckus(config-sys)#
```

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

abort

Exits the config-sys-snmpv2 context without saving changes.

end

Saves changes, and then exits the config-sys-snmpv2 context.

exit

Saves changes, and then exits the config-sys-snmpv2 context.

quit

Exits the config-sys-snmpv2 context without saving changes.

no access-v3

Disables special MIB node for customer's kt.

access-v3

Enables special MIB node for customer's kt.

contact *WORD*

Enables SNMPV2 agent and sets the system contact.

location *WORD*

Enables SNMPV2 agent and sets the system location.

ro-community *WORD*

Enables SNMPV2 agent and sets the RO community name.

rw-community *WORD*

Enables SNMPV2 agent and sets the RW community name.

show

Displays SNMPV2 agent and SNMP trap settings.

Defaults

SNMP Agent:

Status= Enabled

Contact= https://support.ruckuswireless.com/contact_us

Location= 350 West Java Dr. Sunnyvale, CA 94089 US

RO Community= public

RW Community= private

SNMP Trap:

Format= Version2

Status= Disabled

Support-access-V3:

Status= Disabled

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.

Example

```
ruckus(config-sys-snmpv2)# show
SNMP Agent:
  Status= Enabled
  Contact= https://support.ruckuswireless.com/contact_us
  Location= 350 West Java Dr. Sunnyvale, CA 94089 US
  RO Community= public
  RW Community= private

SNMP Trap:
  Format= Version2
  Status= Disabled

Support-access-V3:
  Status= Disabled
```

snmpv2-ap

To enable SNMP AP notification, use the following command:

snmpv2-ap

Example

```
ruckus(config-sys)# snmpv2-ap
The SNMP v2 agent settings have been updated.
ruckus(config-sys)#
```

no snmpv2-ap

To disable SNMP AP notification, use the following command:

no snmpv2-ap

Example

```
ruckus(config-sys)# no snmpv2-ap
The SNMP v2 agent settings have been updated.
ruckus(config-sys)#
```

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

abort

> Exits the config-sys-snmpv3 context without saving changes.

end

> Saves changes, and then exits the config-sys-snmpv3 context.

exit

> Saves changes, and then exits the config-sys-snmpv3 context.

quit

> Exits the config-sys-snmpv3 context without saving changes.

ro-user *WORD*

> Contains commands that can be executed from within the context.

ro-user *WORD* MD5 *WORD*

> Contains commands that can be executed from within the context.

ro-user *WORD* MD5 *WORD* DES *WORD*

> Sets the privacy phrase of DES for SNMPV3.

ro-user *WORD* MD5 *WORD* AES *WORD*

> Sets the privacy phrase of AES for SNMPV3.

ro-user *WORD* MD5 *WORD* None

> Sets the privacy to None for SNMPV3.

ro-user *WORD* SHA *WORD*

> Contains commands that can be executed from within the context.

ro-user *WORD* SHA *WORD* DES *WORD*

> Sets the privacy phrase of DES for SNMPV3.

ro-user *WORD* SHA *WORD* AES *WORD*

> Sets the privacy phrase of AES for SNMPV3.

ro-user *WORD* SHA *WORD*; None

> Sets the privacy to None for SNMPV3.

rw-user *WORD*

> Contains commands that can be executed from within the context.

rw-user *WORD* MD5 *WORD*

      Contains commands that can be executed from within the context.

rw-user *WORD* MD5 *WORD* DES *WORD*

      Sets the privacy phrase of DES for SNMPV3.

rw-user *WORD* MD5 *WORD* AES *WORD*

      Sets the privacy phrase of AES for SNMPV3.

rw-user *WORD* MD5 *WORD* None

      Sets the privacy to None for SNMPV3.

rw-user *WORD* SHA *WORD*

      Contains commands that can be executed from within the context.

rw-user *WORD* SHA *WORD* DES *WORD*

      Sets the privacy phrase of DES for SNMPV3.

rw-user *WORD* SHA *WORD* AES *WORD*

      Sets the privacy phrase of AES for SNMPV3.

rw-user *WORD* SHA *WORD* None

      Sets the privacy to None for SNMPV3.

show

      Displays SNMPV3 agent and SNMP trap settings.

Defaults

SNMPV3 Agent:

Status= Disabled

Ro:

User=

Authentication Type= MD5

Authentication Pass Phrase=

Privacy Type= DES

Privacy Phrase=

Rw:

User=

Authentication Type= MD5

Authentication Pass Phrase=

Privacy Type= DES

Privacy Phrase=

SNMP Trap:

Format= Version3

Status= Disabled

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.

syslog

To enable syslog notifications and enter the config-sys-syslog context, use the following command:

syslog

Example

```
ruckus(config-sys)# syslog
ruckus(config-sys-syslog)#
```

no syslog

To disable syslog notification, use the following command:

no syslog

Syntax Description

no syslog

Disable syslog notification

Defaults

Disabled.

Example

```
ruckus(config-sys)# no syslog
The syslog settings have been updated.
ruckus(config-sys)#
```

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.

Example

```
ruckus(config-sys-syslog)# server 172.17.16.2
The syslog settings have been updated.
ruckus(config-sys-syslog)#
```

type

To set the syslog server type, use the following command:

type <*LOG TYPE*>

Syntax Description

all: Sets remote syslog type to all.

client: Sets remote syslog type to client info.

flowlevel: Sets remote syslog type to flowlevel.

Example

```
ruckus(config-sys-syslog)# type all
The syslog settings have been updated.
ruckus(config-sys-syslog)#
```

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, or keep)

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, or keep).

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)#
```

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** context. These commands must be used from the **config-sys** context.

mgmt-acl

To create or configure a management ACL, use the following command:

mgmt-acl *WORD*

Syntax Description

mgmt-acl

Create or configure a management ACL

WORD

Create or configure this management ACL

Defaults

None.

Usage Guidelines

Executing this command enters the **config-mgmt-acl** context.

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

To delete a management ACL for IPv4, use the following command:

no mgmt-acl *WORD*

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).

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

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

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

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 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

Usage Guidelines

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

Example

```
ruckus(config-sys)# qos
ruckus(config-sys-qos)# show
System QoS:
ToS DATA TUNNEL = 0xA0
ToS CTRL TUNNEL = 0xA0
ToS Classification-Voice = 0xE0 0xC0 0xB8
ToS Classification-Video = 0xA0 0x80
ToS Classification-Data = 0x0
ToS Classification-Background = 0x0
Tx fail threshold = 50
heuristics inter-packet-gap Video = 0   65
heuristics inter-packet-gap Voice = 15 275
heuristics packet-length Video = 1000   1518
heuristics packet-length Voice = 70 400
heuristics classification Video = 50000
heuristics classification Voice = 600
heuristics no classification Video = 500000
heuristics no classification Voice = 10000

ruckus(config-sys-qos)#
```

tunnel-mtu

To set the tunnel MTU, use the following command:

tunnel-mtu *NUMBER*

Syntax Description

tunnel-mtu

Set the tunnel MTU value (850 - 1500)

Defaults

None.

Example

```
ruckus(config-sys)# tunnel-mtu 1500
The Tunnel MTU settings have been updated.
ruckus(config-sys)#
```

> **NOTE**
> You can set tunnel MTU only in Dedicated Master mode.

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)#
```

snmp-trap

To set the SNMP trap format, use the following command:

snmp-trap *[SNPv2 | SNMPv3]*

Syntax Description

snmp-trap

Enable SNMP trap notifications

SNMPv2

Set SNMP trap format to SNMPv2

SNMPv3

Set SNMP trap format to SNMPv3

Example

```
ruckus(config-sys)# snmp-trap SNMPv2
The SNMP trap settings have been updated.
ruckus(config-sys)#
```

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

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

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

Example

```
ruckus(config-sys)# no snmpv3-trap 1
The SNMP trap settings have been updated.
```

no snmpv2

To disable the SNMPv2 agent, use the following command:

no snmpv2

Syntax Description

no snmpv2

Disables the SNMPv2 agent

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

Example

```
ruckus(config-sys)# no snmpv3
The SNMP v3 agent settings have been updated.
```

login-warning

To configure the login warning message, use the following command:

login-warning

Syntax Description

login-warning

> Configure the login warning message.

abort

> Exits the login-warning context without saving changes.

end

> Saves changes, and then exits the login-warning context.

exit

> Saves changes, and then exits the login-warning context.

quit

> Exits the login-warning context without saving changes.

content *WORD*

> Customize login warning content.

Example

```
ruckus(config-sys)# login-warning
ruckus(config-sys-login-warning)# content "Warning, you are logging into equipment belonging to ruckus,
if you are not an authorized user please logout immediately."
The login warning settings have been updated.
ruckus(config-sys-login-warning)# end
The login warning settings have been updated.
Your changes have been saved.
ruckus(config-sys)#
```

no login-warning

To disable the login warning message, use the following command:

no login-warning

event-log-level

To configure the event log level, use the following command:

event-log-level *EVENT LOG LEVEL*

Syntax Description

event-log-level

> **Enter the syslog event log level** *1-3* (1:Critical Events Only, 2:Warning and Critical Events, 3:Show More).

Defaults

2: Warning and Critical Events

Example

```
ruckus# config
You have all rights in this mode.
```

```
ruckus(config)# sys
ruckus(config-sys)# syslog
ruckus(config-sys-syslog)# event-log-level 1
The syslog settings have been updated.
ruckus(config-sys-syslog)#
```

show URL-Filtering-License

To display th current URL Filtering License information, use the following command:

show URL-Filtering-License

Example

```
ruckus(config-sys)# show url-filtering-license
ID: 1
Name: URL Filtering Temporal License
Number of APs: 128
Generated by: URL Filtering Temporal license by Ruckus
Serial number/Unique ID: un9418490011251569244593778
Date to Start :Tue Sep 24 16:23:48 2019

Date to End: Mon Dec 23 15:23:48 2019

Status: active
Detailed: This license is available for 54 days.
ruckus(config-sys)#
```

show internet

To display the current internet status information, use the following command:

show internet

Example

```
ruckus(config-sys)# show internet
Status:          Connected
all port:        OK
    port1:       Up
    port2:       Down
IP status:       OK
    IP:          192.168.0.8
DNS status:      OK
    DNS1:        66.90.130.101
    DNS2:        216.82.201.11
GateWay status:  OK
    GateWay:     192.168.0.1  Up
ruckus(config-sys)#
```

show internet-check

To display the current internet status connection information, use the following command:

show internet-check

Example

```
ruckus(config-sys)# show internet-check
Internet Check:
Company = apple, Enable = 1

Internet Check:
Company = microsoft, Enable = 1

Internet Check:
Company = ruckus, Enable = 1

ruckus(config-sys)#
```

support-entitle

To manually download entitlement file, use the following command:

Syntax

support-entitle

Examples

```
ruckus(config-sys)# support-entitle
OK
ruckus(config-sys)#
```

URL-Filtering-License-Renew

To synchronize the URL Filtering License from the RUCKUS Server, use the following command:

URL-Filtering-License-Renew

Example

```
ruckus(config-sys)# URL-Filtering-License-Renew
OK
ruckus(config-sys)#
```

session-stats-resv

To enable session statistics recording, use the following command:

session-stats-resv

Defaults

Disabled

Example

```
ruckus(config-sys)# session-stats-resv
The session statistics function has been enabled.
ruckus(config-sys)#
```

no session-stats-resv

Use the following command to disable recording of session statistics:

no session-stats-resv

Example

```
ruckus(config-sys)# no session-stats-resv
The session statistics function has been disabled.
ruckus(config-sys)#
```

arc-data-transmission

To enable ARC data transmission, use the following command:

arc-data-transmission

Example

```
ruckus(config-sys)# arc-data-transmission
The ARC data transmission has been enabled.
ruckus(config-sys)#
```

no arc-data-transmission

To disable ARC (application recognition and control) data transmission, use the following command:

no arc-data-transmission

Example

```
ruckus(config-sys)# no arc-data-transmission
The ARC data transmission has been disabled.
ruckus(config-sys)#
```

session-limit-unauth-stats

To enable recording of Layer 2 unauthorized session statistics, use the following command:

session-limit-unauth-stats

Defaults

Enabled

Example

```
ruckus(config-sys)# session-limit-unauth-stats
The limited unauthorized session statistics function has been enabled.
ruckus(config-sys)#
```

no session-limit-unauth-stats

To disable recording of Layer 2 unauthorized session statistics, use the following command:

no session-limit-unauth-stats

eapol-no-retry

To disable retransmission of EAPOL-key (message 3/4 and group key), use the following command:

eapol-no-retry

Example

```
ruckus(config-sys)# eapol-no-retry
Eapol-key retry has been disabled
ruckus(config-sys)#
```

no eapol-no-retry

To enable retransmission of EAPOL-key, use the following command:

no eapol-no-retry

Example

```
ruckus(config-sys)# no eapol-no-retry
Eapol-key retry has been enabled
ruckus(config-sys)#
```

master-protect

To configure Unleashed Master AP protection settings, use the following command:

master-protect

Example

```
ruckus(config-sys)# master-protect
ruckus(config-sys-master-protect)#
  help                  Shows available commands.
  history               Shows a list of previously run commands.
  abort                 Exits the master-protect context without saving changes.
  end                   Saves changes, and then exits the master-protect context.
  exit                  Saves changes, and then exits the master-protect context.
  quit                  Exits the master-protect context without saving changes.
  master-max-sta <NUMBER>
                        Set the max station number in master AP.
  show                  Displays master protection settings.
ruckus(config-sys-master-protect)#
```

cpu-reject-sta

To configure CPU reject value settings for the Master protection, use the following command:

cpu-reject-staNUMBER

Syntax Description

cpu-reject-sta

Configure CPU reject value.

NUMBER

Set the headroom CPU utlization threshold value (0~100).

Defaults

3

Example

```
ruckus(config-sys-master-protect)# cpu-reject-sta 85
The master AP protection settings have been updated.
ruckus(config-sys-master-protect)#
```

master-max-sta

To configure Master max station value for the Master protection, use the following command:

cpu-reject-sta*NUMBER*

Syntax Description

cpu-reject-sta

Configure max APs for Master protection.

NUMBER

Set the max APs (0~100).

Defaults

100

Example

```
ruckus(config-sys-master-protect)# master-max-sta 85
The master AP protection settings have been updated.
ruckus(config-sys-master-protect)#
```

generate-token

To Re-generate unleashed-network unique token, use the following command:

generate-token

Example

```
ruckus(config-sys)# generate-token
new-token: un9418490011251346969169799
ruckus(config-sys)#
```

gateway-mode

Use the following command to configure the dual WAN ports for the Unleashed gateway.

gateway-mode

Syntax Description

help

Shows available commands.

history

Shows a list of previously run commands.

abort

Exits the config-sys-gateway context without saving changes.

end

Save changes, and then exits the config-sys-gateway context.

exit

Save changes, and then exits the config-sys-gateway context.

quit

Exits the config-sys-gateway context without saving changes.

no

Contains commands that can be executed from within the context.

wan-port *WORD*

Sets the port number for primary WAN port.

standby-wan-port *WORD*

Sets the port number for standby WAN port.

show

Displays the settings in gateway mode.

Example

```
ruckus(config)# system
ruckus(config-sys)# gateway-mode

    // show port info
    wan-port 1
ruckus(config-sys-gateway-wan):
```

```
            ip mode: dhcp
                    dhcp    static pppoe
            ip addr <IPADDR> <NETMASK>
            ip route gateway <GWADDR>
            ip name-server {DNSADDR} [{DNSADDR2}]
            pppoe user-name <username> password <password>

            lan ip addr <IPADDR> <NETMASK>
            lan ip name-server <DNS-ADDR> <DNS-ADDR>
            lan ip-range <IPADDR> <IPADDR>
            lan lease-time: 6-hours|12-hours|1-day|2-days|1-week|2-weeks;

            show
ruckus(config-sys-gateway):
    // show port info
    standby-wan-port 2:
    no standby-wan-port:

ruckus(config-sys-gateway-standby-wan):
        ip mode: dhcp
                dhcp static
        ip addr <IPADDR> <NETMASK> gateway <GWADDR>
          ip name-server {DNSADDR} [{DNSADDR2}]
ruckus(config-sys-gateway)#
```

show

To display config-sys current settings, use the following command:

show

Example

```
ruckus(config-sys)# show
Country Code:
  Code= United States

Internet Check:
Company = apple, Enable = 1

Internet Check:
Company = microsoft, Enable = 1

Internet Check:
Company = ruckus, Enable = 1

Identity:
  Name= Ruckus-Unleashed

Session Statistics:
  Enable= false
  Limited Unauthorized Session= true

ARC Data Transmission:
  Enable= true

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

Log:
  Status= Disabled
  Address=
  Type=
  Facility=
  Priority=
  AP Facility=
  AP Priority=
  event log level= 1

Bonjour Service:
  Status= Enabled

Telnet Server:
  Status= Disabled

FTP Server:
  Status= Enabled
  Anonynous Status= Disabled

Unleashed Multi-Site Manager:
  Status= Disabled
  Address=
  Interval= 3

login warning:
  Status= Disabled
  content= "Warning, you are logging into device for authorized user only. If
yo                                                               u are not an
authorized user, please click Quit; otherwise click Continue to
log                                                              in."

LWAPP:
```

```
    MGMT queue length threshold to drop AUTH frame = 100
    MGMT queue length threshold to resume processing AUTH frame = 25

EAPoL Key no Retry:
  Status= Disabled

Unleashed Network:
  Token= un9418490011251529244593778

ruckus(config-sys)#
```

Configure UPNP Settings

Use the following commands to enable or disable Universal Plug and Play:

upnp

upnp

Syntax Description

upnp

Enable UPnP

Defaults

Enabled.

Example

```
ruckus(config)# upnp
UPnP Service is enabled
/bin/upnp enable
ruckus(config)#
```

no upnp

no upnp

Syntax Description

no upnp

Enable UPnP

Defaults

Enabled.

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-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)#
```

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)#
```

> **NOTE**
> You can create a maximum of 16 WLANs in non-Dedicated mode and 64 WLANs in Dedicated mode.

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)#
```

wlan-bind

Enables WLAN binding on the 2.4 GHz, 5 GHz, 6 GHz, or all the radios.

Syntax

wlan-bind { **2.4** | **5** | **6**| **all** }

no wlan-bind { **2.4** | **5** | **6**|**all** }

Command Default

WLAN binding is enabled on all the radios.

Parameters

2.4

Specifies the 2.4 GHz radio.

5

Specifies the 5 GHz radio.

6

Specifies the 6 GHz radio.

all

Specifies all radios.

Modes

WLAN configuration mode

Usage Guidelines

Use the **show wlan all** command to display information about the WLAN bind from the User EXEC mode.

The **no** form of the command removes the configured wlan bind values for the radio(s).

Examples

The following example enables WLAN binding on all radios.

```
ruckus# config
ruckus(config)# wlan testwlan33
ruckus(config-wlan)# wlan-bind all
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)# exit
ruckus(config)# exit
ruckus# show wlan all
WLAN Service:
ID:
1:
NAME = Ruckus1
Tx. Rate of Management Frame(2.4GHz) = 2.0Mbps
Tx. Rate of Management Frame(5GHz) = 6.0Mbps
Beacon Interval = 100ms
SSID = Ruckus1
Description = Ruckus1
Type = Standard Usage
Authentication = open
Encryption = wpa2
Algorithm = aes
Passphrase = secretpassphrasegoeshere
FT Roaming = Disabled
802.11k Neighbor report = Disabled
Web Authentication = Disabled
Authentication Server = Disabled
Accounting Server = Disabled
Called-Station-Id type = wlan-bssid
Tunnel Mode = Disabled
DHCP relay = Disabled
Max. Clients = 100
Isolation per AP = Disabled
Isolation across AP = Disabled
Zero-IT Activation = Enabled
Load Balancing = Disabled
Band Balancing = Disabled
Wifi6 = Enabled
Service = Enabled
Dynamic PSK = Enabled
Dynamic PSK Passphrase Length =
Dynamic PSK Expire Time = unlimited
Dynamic PSK Validity Period =
Limit Dynamic PSK = Disabled
Auto-Proxy configuration:
Status = Disabled
Inactivity Timeout:
Status = Disabled
VLAN-ID = 1
Dynamic VLAN = Disabled
Closed System = Disabled
Https Redirection = Disabled
OFDM-Only State = Disabled
Multicast Filter State = Disabled
802.11d State = Disabled
Force DHCP State = Disabled
Force DHCP Timeout = 0
DHCP Option82:
Status = Disabled
Option82 sub-Option1 = Disabled
Option82 sub-Option2 = Disabled
Option82 sub-Option150 = Disabled
Option82 sub-Option151 = Disabled
Ignore unauthorized client statistic = Disabled
STA Info Extraction State = Enabled
BSS Minrate = Disabled
DTIM period = 1
Directed MC/BC Threshold = 5
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 = No ACLS
Proxy ARP = Disabled
Device Policy = No ACLS
Vlan Pool = No Pools
Role based Access Control Policy = Disabled
SmartRoam = Disabled Roam-factor = 1
Allow List = No ACLS
Application Recognition & Control = Disabled
Apply ARC Policy = NO POLICY
Wlan Bind = all
Client Flow Data Logging = Disabled
Client Connection Data = Disabled
ruckus#
```

History

Release version	Command history
200.16	This command was modified to include the 6 GHz radio setting.

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* | **autonomous**]

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

autonomous

> Set the WLAN type to Autonomous.

Defaults

Standard usage

Example

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

type standard-usage

To set the WLAN type to "Standard Usage", use the following command:

type standard-usage

type standard

type guest-access

To set the WLAN type to "Guest Access", use the following command:

type guest-access *WORD*

Example

```
ruckus(config-wlan)# type guest-access guestpolicy1
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

type hotspot

To set the WLAN type to "Hotspot", use the following command:

type hotspot

type hs20

To set the WLAN type to "Hotspot 2.0", use the following command:

type hs20<*WORD*>

Syntax Description

type hs20: set WLAN type to Hotspot 2.0

<WORD>: set Hotspot 2.0 Operator name

Example

```
ruckus(config-wlan)# type hs20 operator1
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

open

To set the authentication method to 'open', use the following command:

open [none|owe|wpa2|wpa3|wpa23-mixed|wpa-mixed] passphrase <WORD> algorithm <WORD>]

Syntax Description

- none: Sets the authentication method to 'open' and encryption method to 'none'.
- owe: Sets the authentication method to 'open', encryption method to 'OWE', algorithm to 'AES', and pmf to 'required'.
- wpa2: Sets the authentication method to 'open' and encryption method to 'WPA2'.

- wpa3: Sets the authentication method to 'open' and encryption method to 'WPA3'.

- wpa23-mixed: Sets the encryption method to 'WPA2/WPA3 Mixed'.

- wpa-mixed: Sets the encryption method to 'WPA/WPA2 Mixed'.

- AES: Sets the algorithm to AES.

- auto: Sets the algorithm to auto.

Defaults

None.

Example

```
ruckus(config)# wlan wlan2
The WLAN service 'wlan2' has been created. To save the WLAN service, type 'end' or 'exit'.
ruckus(config-wlan)# open none
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)# end
The WLAN service 'wlan2' has been updated and saved.
Your changes have been saved.
ruckus(config)#
```

open owe

To set the authentication method to 'open', encryption method to 'OWE', algorithm to 'AES', and pmf to 'required', use the following command:

open owe

Example

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

open wpa2

To set the authentication method to 'open' and encryption method to 'WPA2', use the following command:

open wpa2 passphrase *WORD* algorithm *[aes|auto]*

Example

```
ruckus(config-wlan)# open wpa2 passphrase pass1234 algorithm aes
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

open wpa3

To set the encryption method to WPA3, use the following command:

open wpa3 passphrase <PASSPHRASE> algorithm *aes*

Example

```
ruckus(config-wlan)# open wpa3 passphrase pass1234 algorithm aes
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

open wpa23-mixed

To set the encryption method to 'WPA2/WPA3 Mixed', use the following command:

open wpa23-mixed psk-passphrase *<PASSPHRASE>* sae-passphrase *<PASSPHRASE>* algorithm *AES*

Example

```
ruckus(config-wlan)# open wpa23-mixed psk-passphrase pass1234 sae pass5678 algorithm aes
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

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'.
```

Configure Dynamic PSK Commands

Use the following commands to enable and configure RUCKUS Dynamic Pre-Shared Key functionality for the WLAN.

dynamic-psk enable

To enable internal Dynamic Pre-Shared Keys, use the following command:

dynamic-psk enable

Syntax Description

dynamic-psk enable
> Enable internal Dynamic PSK

Defaults

Disabled

Example

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

no dynamic-psk

To disable Dynamic Pre-Shared Keys on the WLAN, use the following command:

no dynamic-psk

dynamic-psk external

To enable external dynamic PSK and set the authentication server to external DPSK, use the following command:

dynamic-psk external auth-server*<WORD>*

Command Syntax

dynamic-psk external: set DPSK server to external.

auth-server: designate the external authentication server name.

<WORD>: name of the authentication server.

Example

```
ruckus(config-wlan)#dynamic-psk external auth-server radius1
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*

dynamic-psk type

To sets the type of dynamic PSK (secure, mobile friendly, or user friendly), use the following command:

dynamic-psk type [mobile-friendly|secure|numeral]

Syntax Description

dynamic-psk type

Set the DPSK type

mobile-friendly

Set the DPSK type to mobile friendly

secure

Set the DPSK type to secure

numeral

Sets the dynamic PSK type to user friendly (number only)

Defaults

Secure

Example

```
ruckus(config-wlan)# dynamic-psk type mobile-friendly
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

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

shared-dpsk

To enable Shared Dynamic PSK and set the number of device that shared one unbound DPSK, use the following command:

shared-dpsk<*NUMBER*>

Command Syntax

shared-dpsk: enable shared DPSK.

<*NUMBER*>: enter a number of devices which share one unbound DPSK.

Example

```
ruckus(config-wlan)# shared-dpsk 40
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

no shared-dpsk

To disable shared Dynamic PSK, use the following command:

no shared-dpsk

Command Syntax

no shared-dpsk: disable shared DPSK.

Example

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

dynamic-psk-expiration

To set the WLAN Dynamic PSK expiration, use the following command:

dynamic-psk-expiration [**length** | **start-point**] *WORD*

Syntax Description

dynamic-psk-expiration

Sets the DPSK expiration.

length

Sets the DPSK expiration length.

unlimited

Sets wlan dynamic psk expiration to unlimited.

one-day

Sets wlan dynamic psk expiration to one day.

one-week

Sets wlan dynamic psk expiration to one week.

two-weeks

Sets wlan dynamic psk expiration to two weeks.

one-month

Sets wlan dynamic psk expiration to one month.

two-months

Sets wlan dynamic psk expiration to two months.

three-months

Sets wlan dynamic psk expiration to three months.

half-a-year

Sets wlan dynamic psk expiration to half a year.

one-year

Sets wlan dynamic psk expiration to one year.

two-years

Sets wlan dynamic psk expiration to two years.

start-point

Sets the DPSK validity start-point.

first-use

The D-PSK expiration will be calculated from when it is first used.

creation-time

The D-PSK expiration will be calculated from when it is created.

Example

```
ruckus(config-wlan)# dynamic-psk-expiration start-point first-use
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)# dynamic-psk-expiration length one-week
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

mac none

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)# mac none auth-server Ruckus-Auth-01
The command was executed successfully.
ruckus(config-wlan)#
```

mac owe

To set the authentication to MAC address and encryption method to 'OWE', use the following command:

mac owe auth-server *<WORD>*

Example

```
ruckus(config-wlan)# mac owe auth-server radius1
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

dot1x

To set the authentication method to '802.1x EAP', use the following command:

dot1x [wpa2| wpa3| wpa23-mixed]algorithm[aes|AES-GCMP-256auth-server[local|name*<WORD>*]

Command Syntax

dot1x: set auth method to dot1x.

wpa2: set the encryption method to WPA2.

wpa3: set the encryption method to WPA3.

wpa23-mixed: set the encryption method to WPA2/WAP3-Mixed.

algorithm: define the encryption algorithm.

aes: set the encryption algorithm to "AES".

AES-GCMP-256: set the encryption algorithm to "AES-GCMP-256".

auth-server: designate the authentication server.

local: Sets the authentication server to 'Local Database'.

name: Sets the authentication server to the specified name from AAA.

<WORD>: name of the external authentication server.

Example

```
ruckus(config-wlan)# dot1x wpa2 algorithm aes auth-server local
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

dot1x wpa2

To set the authentication method to '802.1x EAP', encryption method to 'WPA2', and algorithm to 'AES', use the following command:

dot1x wpa2algorithm 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)# dot1x wpa2 algorithm AES auth-server Ruckus-RADIUS
The command was executed successfully.
ruckus(config-wlan)#
```

dot1x wpa3

To set the authentication method to 802.1X and the encryption method to WPA3, use the following command:

dot1x wpa3 algorithm AES-GCMP-256 auth-server name*<WORD>*

Defaults

None

Example

```
ruckus(config-wlan)# ruckus(config-wlan)# dot1x wpa3 algorithm AES-GCMP-256 auth-server name radius1
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

dot1x wpa2/wpa3-mixed

To set the authentication method to "802.1x EAP", encryption method to "WPA2/WPA3-Mixed", and algorithm to "AES", use the following command:

dot1x wpa23-mixed algorithm AES auth-server [**local**|**name***<WORD>*]

Syntax Description

dot1x

Set the authentication method to 802.11x

wpa23-mixed

Set the encryption method to WPA2/WPA3-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)# dot1x wpa23-mixed algorithm AES auth-server Ruckus-RADIUS
The command was executed successfully.
ruckus(config-wlan)#
```

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 (per-AP or across APs), use the following command:

client-isolation [**isolation-on-ap** | **isolation-on-subnet**] [**enable** | **disable**]

Syntax Description

client-isolation

> Enable client isolation for this WLAN.

isolation-on-ap

> Enable client isolation per AP.

isolation-on-subnet

> Enable client isolation across APs.

Example

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

allowlist

To apply a client isolation allowlist to this WLAN, use the following command:

allowlist name *WORD*

no allowlist

To disable the allowlist for this WLAN, use the following command:

no allowlist

load-balancing

To enable load balancing for this WLAN, use the following command:

load-balancing

Defaults

Disabled

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

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

band-balancing

To enable band balancing for this WLAN, use the following command:

band-balancing

Defaults

Enabled.

Example

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

no band-balancing

To disable band balancing for this WLAN, use the following command:

no band-balancing

send-eap-failure

To enable send EAP failure messages, use the following command:

send-eap-failure

Defaults

Disabled

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

```
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

Defaults

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)#
```

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)# web-auth Ruckus-RADIUS
The command was executed successfully.
ruckus(config-wlan)#
```

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)# no web-auth
The command was executed successfully.
```

grace-period

To enable and set a maximum time (in minutes) for which users must re-authenticate after disconnecting, 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, use the following command:

no grace-period *NUMBER*

Syntax Description

no grace-period

Disables the 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)# 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)# 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

Configuring Master Settings
Configure WLAN Settings Commands

Defaults

None.

Example

```
ruckus# config
ruckus(config)# wlan wlan-123
ruckus(config-wlan)# no acct-server
The command was executed successfully.
```

inactivity-timeout

To set the inactivity timeout to the specified number in minutes, use the following command:

inactivity-timeout *NUMBER*

Syntax Description

inactivity-timeout

Enable and set the inactivity timeout

NUMBER

Set the inactivity timeout in minutes (1-500 min.)

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)#
```

web-auth-timeout

To enable and set the web authentication timeout time to the specified number in minutes, use the following command:

web-auth-timeout *NUMBER*

Syntax Description

web-auth-timeout

Enable and set the web authentication timeout

NUMBER

Set the inactivity timeout in minutes

Defaults

5

Example

```
ruckus(config-wlan)# web-auth-timeout 15
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

vlan

To set the VLAN ID for the WLAN, use the following command:

vlan *NUMBER*

Syntax Description

vlan

Enable VLAN

NUMBER

Set the VLAN ID to this value

Defaults

1

Example

```
ruckus(config-wlan)# vlan 123
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

dynamic-vlan

To enable dynamic VLAN, use the following command:

dynamic-vlan

Syntax Description

dynamic-vlan

Enable dynamic VLAN

Usage Guidelines

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

Disabled

Example

```
ruckus# config
ruckus(config)# wlan wlan-123
```

```
ruckus(config-wlan)# 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

Disabled

Example

```
ruckus# config
ruckus(config)# wlan wlan-123
ruckus(config-wlan)# 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

transient-client-management

To enable transient client management, use the following command:

transient-client-management

Defaults

Disabled.

Example

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

no transient-client-management

To disable transient client management, use the following command:

no transient-client-management

Defaults

Disabled.

Example

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

join-wait-time

To set the time to wait on join requests (1-60 seconds, 5 by default), use the following command:

join-wait-time *<NUMBER>*

Defaults

5

Example

```
ruckus(config-wlan)# transient-client-management
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#   join-wait-time 5
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

join-wait-threshold

To set the number of join requests to wait (1-50 seconds, 5 by default), use the following command:

join-wait-threshold *<NUMBER>*

Defaults

5

Example

```
ruckus(config-wlan)# join-wait-threshold 5
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

join-expire-time

To set the join expire time (1-300 seconds, 300 by default), use the following command:

join-expire-time *<NUMBER>*

Defaults

300

Example

```
ruckus(config-wlan)# join-expire-time 300
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

min-client-rssi

To set the minimum client RSSI threshold (-90 to -60 dBm, -85 by default), use the following command:

min-client-rssi *<NUMBER>*

Defaults

-85

Example

```
ruckus(config-wlan)# min-client-rssi -85
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

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

dtim-period

To set the DTIM period of the WLAN, use the following command:

dtim-period *NUMBER*

Syntax Description

dtim-period

Sets the DTIM period of the WLAN (1-255).

NUMBER

DTIM period.

Defaults

1

Example

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

no dtim-period

To set the DTIM period of the WLAN to 1 (default), use the following command:

no dtim-period

Syntax Description

no dtim-period

Set the DTIM period to 1.

Defaults

1

Example

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

directed-threshold

To set the Directed MC/BC threshold of the WLAN (0-128), use the following command:

directed-threshold *NUMBER*

Syntax Description

directed-threshold

Set the Directed MC/BC threshold of the WLAN.

NUMBER

Directed threshold (0-128)

Defaults

5

Example

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

no directed-threshold

To set the Directed MC/BC threshold of the WLAN to 5 (default), use the following command:

no directed-threshold

Syntax Description

no directed-threshold

Sets the Directed Multicast/Broadcast threshold to 5.

Defaults

5

Example

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

smart-roam

To enable and set SmartRoam with the specified roam factor (1-10), use the following command:

smart-roam *NUMBER/EMPTY*

no smart-roam

To disable the SmartRoam feature, use the following command:

no smart-roam

force-dhcp

To enable the Force DHCP option, use the following command:

force-dhcp

Defaults

Disabled

Example

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

force-dhcp-timeout

To disconnect the client if it does not obtain valid IP address within the specified timeout period (in seconds), use the following command:

force-dhcp-timeout *NUMBER*

Defaults

10 seconds

Example

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

no force-dhcp

To disable the Force DHCP option, use the following command:

no force-dhcp

sta-info-extraction

To enable station information extraction (client fingerprinting), use the following command:

sta-info-extraction

Defaults

Enabled

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

100

Example

```
ruckus(config-wlan)# max-clients 100
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

802dot11d

To enable 802.11d for the WLAN, use the following command:

802dot11d

Defaults

Enabled

no 802dot11d

To disable 802.11d for the WLAN, use the following command:

no 802dot11d

arc

Use the following command to enable Application Recognition & Control:

arc

Defaults

Disabled

Example

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

no arc

Use the following command to disable Application Recognition and Control:

no arc

apply-arc-policy

Use the following command to apply an application policy to the WLAN:

apply-arc-policy *WORD*

Defaults

None

Example

```
ruckus(config-wlan)# apply-arc-policy facebook
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

no apply-arc-policy

Use the following command to disable an application policy for the WLAN:

no apply-arc-policy

Defaults

None

Example

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

wifi-calling

To enable Wi-Fi Calling with the specified profile, enter the following command:

wifi-calling enable profile *<WORD>*

Defaults

Disabled.

Example

```
ruckus(config-wlan)# wifi-calling enable profile profile1
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

no wifi-calling

To disable Wi-Fi Calling for the WLAN, enter the following command:

no wifi-calling

Defaults

Disabled.

Example

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

url-filtering

To enable URL Filtering for the WLAN, use the following command:

url-filtering

Defaults

Disabled

Example

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

no url-filtering

To disable URL Filtering for the WLAN, use the following command:

no url-filtering

Defaults

Disabled

Example

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

url-filtering-profile

Use the following command to apply a URL filtering profile to the WLAN:

url-filtering-profile *WORD*

Defaults

None

Example

```
ruckus(config-wlan)# url-filtering-profile filter1
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

sae-anti-clogging-threshold

To set the SAE anti_clogging_threshold to the specified number, use the following command:

sae-anti-clogging-threshold<NUMBER>

Defaults

None

Example

```
ruckus(config-wlan)# sae-anti-clogging-threshold 10
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

roaming-acct-interim-update

To enable accounting interim-updates when a client roams, use the following command:

roaming-acct-interim-update

Defaults

Disabled.

Usage Guidelines

When "roaming-acct-interim-update" is set, all traffic and session-id data from the original session is carried over to the new session.

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

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.

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'.
```

acl

To configure an L2 MAC/L3/L4/IP ACL with the specified name, use the following command:

Syntax

acl [**l2acl** | **dvcpcy** | **prece**| **role-based-access-ctrl**| **l3acl**} *<WORD>*]

Parameters

l2acl

Configures a L2 ACL with the specified name.

dvcpcy

Configures a Device Policy with the specified name.

prece

Configures a Precedence Policy with the specified name.

role-based-access-ctrl

Enable Role based Access Control Policy.

l3acl

Configures a L3/L4/IP ACL with the specified name.

<WORD>

Specify the name of the ACL.

Examples

```
ruckus(config-wlan)# acl l2acl acl1
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

acl role-based-access-ctrl

To enable Role based Access Control Policy on the WLAN, use the following command:

acl role-based-access-ctrl

Defaults

Disabled

Example

```
ruckus(config-wlan)# acl role-based-access-ctrl
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

no role-based-access-ctrl

To disable role based access control policy service, use the following command:

no role-based-access-ctrl

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

acl prece

To apply a Precedence Policy to the WLAN, use the following command:

acl prece *WORD*

acl dvcpcy

To apply a Device Policy to the WLAN, use the following command:

acl dvcpcy *WORD*

no dvcpcy

To disable device policy for this WLAN, use the following command:

no dvcpcy

mac-addr-format

Sets MAC auth username and password to one of the following formats:

mac-addr-format aa-bb-cc-dd-ee-ff

Sets MAC auth username and password to format aa-bb-cc-dd-ee-ff.

mac-addr-format aa:bb:cc:dd:ee:ff

Sets MAC auth username and password to format aa:bb:cc:dd:ee:ff.

mac-addr-format AABBCCDDEEFF

Sets MAC auth username and password to format AABBCCDDEEFF.

mac-addr-format AA-BB-CC-DD-EE-FF

Sets MAC auth username and password to format AA-BB-CC-DD-EE-FF.

mac-addr-format AA:BB:CC:DD:EE:FF

Sets MAC auth username and password to format AA:BB:CC:DD:EE:FF.

no mac-addr-format

Sets MAC auth username and password to format aabbccddeeff.

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

80211w-pmf

To enable 802.11w PM, use the following command:

80211w-pmf

no 80211w-pmf

To disable 802.11w PMF, use the following command:

no 80211w-pmf

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

ft-roaming

To enable FT Roaming, use the following command:

ft-roaming

Example

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

no ft-roaming

To disable FT Roaming, use the following command:

no ft-roaming

rrm-neigh-report

To enable 802.11k Neighbor-list report, use the following command:

rrm-neigh-report

Example

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

no rrm-neigh-report

To isable 802.11k Neighbor-list report, use the following command:

no rrm-neigh-report

https-redirection

To enable HTTPS redirection, use the following command:

https-redirection

no https-redirection

To disable HTTPS redirection, use the following command:

no https-redirection

client-flow-log

To enable logging of client flow data to external syslog, use the following command:

client-flow-log

Example

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

no client-flow-log

To disable logging of client flow data to external syslog, use the following command:

no client-flow-log

Example

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

client-connect-log

To enable logging of client connect data, use the following command:

client-connect-log

Defaults

Disabled

Example

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

no client-connect-log

To disable logging of client connection data, use the following command:

client-connect-log

Defaults

Disabled

Example

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

bypasscna

Use the following command to bypass Apple Captive Network Assistance (CNA) on iOS and OS X devices.

bypasscna

Example

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

no bypasscna

To disable the bypass Apple CNA feature, use the following command:

no bypasscna

Example

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

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:
    1:
      NAME = Ruckus-Wireless-1
      Tx. Rate of Management Frame(2.4GHz) = 2.0Mbps
      Tx. Rate of Management Frame(5GHz)   = 6.0Mbps
      Beacon Interval = 100ms
      SSID = Ruckus-Wireless-1
      Description = Ruckus-Wireless-1
      Type = Standard Usage
      Authentication = open
      Encryption = wpa
      Algorithm = aes
      Passphrase = password
      FT Roaming = Disabled
      802.11k Neighbor report = Disabled
      Web Authentication = Disabled
      Authentication Server = Disabled
      Accounting Server = Disabled
      Called-Station-Id type = wlan-bssid
      Tunnel Mode = Disabled
      DHCP relay = Disabled
      Max. Clients = 100
      Isolation per AP = Disabled
      Isolation across AP = Disabled
      Zero-IT Activation = Enabled
      Load Balancing = Disabled
      Band Balancing = Disabled
      Wifi6 = Enabled
      Service = Enabled
      Dynamic PSK = Enabled
      Dynamic PSK Passphrase Length =
      Limit Dynamic PSK = Disabled
      Auto-Proxy configuration:
        Status = Disabled
      Inactivity Timeout:
          Status = Disabled
      VLAN-ID = 1
      Dynamic VLAN = Disabled
      Closed System = Disabled
      OFDM-Only State = Disabled
      Multicast Filter State = Disabled
      802.11d State = Disabled
      Force DHCP State = Disabled
      Force DHCP Timeout = 0
      DHCP Option82:
          Status = Disabled
          Option82 sub-Option1 = Disabled
          Option82 sub-Option2 = Disabled
```

```
        Option82 sub-Option150 = Disabled
        Option82 sub-Option151 = 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 = No ACLS
    Proxy ARP = Disabled
    Device Policy = No ACLS
    Role based Access Control Policy = Disabled
    SmartRoam = Disabled   Roam-factor = 1
    Allow List = No ACLS
    Application Visibility = disabled
    Apply Policy Group = No_Denys


  ruckus(config)#
```

wifi6/7

Enables wifi6/7 mode on a WLAN.

Syntax

wifi6/7

no wifi6/7

Command Default

By default, wifi6/7 mode is enabled.

Modes

WLAN configuration mode

Usage Guidelines

The 6 GHz radio will become non-operational if wifi6/7 mode is disabled.

The **no** form of the command disables wifi6/7 mode on the specified WLAN.

Examples

The following example enables the wifi6/7 mode on a WLAN.

```
ruckus# config
ruckus(config)# wlan testwlan2
ruckus(config-wlan)# wifi6/7
The command was executed successfully. To save the changes, type 'end' or 'exit'.
WLAN Service:
  ID:
……
Wifi6/7 = Enabled
ruckus(config-wlan)#
```

The following example disables the wifi6/7 mode on a WLAN.

```
ruckus# config
ruckus(config)# wlan testwlan2
ruckus(config-wlan)# no wifi6/7
The command was executed successfully. To save the changes, type 'end' or 'exit'.
WLAN Service:
  ID:
……
Wifi6/7 = Disabled
ruckus(config-wlan)#
```

History

Release version	Command history
200.11	This command was introduced.
200.16	This command was modified to include the wifi7 option.

service

To enable WLAN service, use the following command:

service

Syntax Description

service

        Enable WLAN service.

Example

```
ruckus(config)# wlan wlan_aaa
The WLAN service 'wlan_aaa' has been loaded. To save the WLAN service, type 'end' or 'exit'.
ruckus (config-wlan)# service
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus (config-wlan)#
ruckus (config-wlan)# show
WLAN Service:
NAME = wlan_aaa
…
Service = Enabled
…
```

no service

To disable WLAN service, use the following command:

no service

Example

```
ruckus(config-wlan)# no service
The command was executed successfully. To save the changes, type 'end' or 'exit'.
WLAN Service:
NAME = wlan_aaa
…
Service = Disabled
…
```

guess-friendly-key

To enable guest friendly key, use the following command:

guess-friendly-key

Syntax Description

guess-friendly-key

        Enables guest friendly key.

Example

```
ruckus(config-wlan)# guess-friendly-key
Enables Guest Friendly Key
```

no guess-friendly-key

To disable guest friendly key, use the following command:

no guess-friendly-key

Example

```
ruckus(config-wlan)# no guess-friendly-key
Disables Guest Friendly Key
```

tunnel-mode

To enable tunnel mode, use the following command:

tunnel-mode

Syntax Description

tunnel-mode
> Enable tunnel mode

Defaults

Disabled.

Example

```
ruckus# config
ruckus(config)# wlan wlan-123
ruckus(config-wlan)# tunnel-mode
The command was executed successfully.
```

> **NOTE**
> Tunnel mode can be enabled or disabled when the controller is in Dedicated mode.

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

Disabled.

Example

```
ruckus# config
ruckus(config)# wlan wlan-123
ruckus(config-wlan-wlan-123)# no tunnel-mode
The command was executed successfully.
```

smart-roam

To enable smart roam, use the following command:

ruckus(config-wlan)# smart-roam

Syntax Description

smart-roam

> Enable smart roam

Defaults

Disabled.

Example

```
ruckus# config
ruckus(config)# wlan wlan-123
ruckus(config-wlan)# smart-roam
The command was executed successfully.
ruckus(config-wlan)# show
SmartRoam = Disabled  Roam-factor = 1
```

no smart-roam

To disable smart roam, use the following command:

no smart-roam

Syntax Description

no smart-roam

> Disable smart roam

Defaults

Disabled.

Example

```
ruckus# config
ruckus(config)# wlan wlan-123
ruckus(config-wlan-wlan-123)# no smart-roam
The command was executed successfully.
```

bss-priority

Sets the WLAN Basic Service Set (BSS) priority level.

Syntax

bss-priority { **high** | **low** }

Command Default

By default, all WLANs are set to high priority.

Parameters

high

Configures the WLAN BSS priority to high.

low

Configures the WLAN BSS priority to low.

Modes

WLAN configuration mode

Usage Guidelines

Setting the WLAN BSS priority to low limits the throughput to all clients connected to this WLAN.

Examples

The following example configures the BSS priority on a WLAN.

```
ruckus# config
ruckus(config)# wlan testwlan1
ruckus(config-wlan)# bss-priority low
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

History

Release version	Command history
200.16	This command was modified to include the "bss" keyword.

qos mirroring

Configures the Quality of Service (QoS) mirroring priority for a WLAN.

Syntax

qos-mirroring *number*

Command Default

By default, QoS mirroring is enabled by protocol.

Parameters

number

0: Disables QoS mirroring

1: Enables via protocol (clients with Mirrored Stream Classification Service (MSCS) requests will have mirrored flows)

2: Enables for All (QoS mirroring is enabled for all the clients on an AP)

Modes

WLAN configuration mode

Examples

The following example configures QoS mirroring on an AP.

```
ruckus# config
ruckus(config)# wlan ruckus12
ruckus(config-wlan)# qos-mirroring 2
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

History

Release version	Command history
200.16	This command was introduced.

transition-disable

Enables the Transition Disable setting on a WPA3 WLAN.

Syntax

transition-disable

no transition-disable

Command Default

By default, transition-disable is disabled.

Modes

WLAN configuration mode

Usage Guidelines

The Transition Disable setting is valid only on WPA3 WLANs.

The **no** form of the command disables the setting.

Examples

The following example enables the Transition Disable setting on a WLAN.

```
ruckus# config
ruckus(config)# wlan testwlan32
ruckus(config-wlan)# transition-disable
The command was executed successfully. To save the changes, type 'end' or 'exit'.
Transition Disable = Enabled
ruckus(config-wlan)#
```

The following example disables the Transition Disable setting on a WLAN.

```
ruckus# config
ruckus(config)# wlan testwlan30
ruckus(config-wlan)# no transition-disable
The command was executed successfully. To save the changes, type 'end' or 'exit'.
Transition Disable = Disabled
ruckus(config-wlan)#
```

History

Release version	Command history
200.16	This command was introduced.

Configure WLAN Group 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 wlangroup2
The WLAN group 'wlangroup2' has been created. To save the WLAN group, type 'end' or 'exit'.
ruckus(config-wlangrp)#
```

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 wlangroup2
The WLAN group 'wlangroup2' has been created. To save the WLAN group, type 'end'  or 'exit'.
ruckus(config-wlangrp)# abort
No changes have been saved.
ruckus(config)#
```

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 wlangroup2
The WLAN group 'wlangroup2' has been created. To save the WLAN group, type 'end' or 'exit'.
ruckus(config-wlangrp)# end
The WLAN group 'wlangroup2' has been updated.
Your changes have been saved.
ruckus(config)#
```

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 wlangroup2
The WLAN group entry 'wlangroup2' has been loaded. To save the WLAN group, type 'end' or 'exit'.
ruckus(config-wlangrp)# exit
The WLAN group 'wlangroup2' has been updated.
Your changes have been saved.
ruckus(config)#
```

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 wlangroup2
The WLAN group entry 'wlangroup2' has been loaded. To save the WLAN group, type 'end' or 'exit'.
ruckus(config-wlangrp)# quit
No changes have been saved.
ruckus(config)#
```

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 *WORD*

Syntax Description

name

> Configure the WLAN group name

WORD

> Set the WLAN group name to this value

Defaults

None.

Example

```
ruckus# config
ruckus(config)# wlan-group wlangroup2
The WLAN group entry 'wlangroup2' has been loaded. To save the WLAN group, type 'end' or 'exit'.
ruckus(config-wlangrp)# name wlangroup2
ruckus(config-wlangrp)# show
WLAN Group:
  ID:
    2:
      Name= wlangroup2
      Description=
      WLAN Service:

ruckus(config-wlangrp)#
```

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. Multiple word text must be enclosed in quotes.

description *WORD*

Syntax Description

description

> Configure the WLAN group description

WORD

> Set the WLAN group description to this value

Defaults

None.

Example

```
ruckus# config
ruckus(config)# wlan-group wlangroup2
ruckus(config-wlangrp)# description "WLAN Group 2"
ruckus(config-wlangrp)# show
WLAN Group:
  ID:
    2:
      Name= wlangroup2
      Description= WLAN Group 2
      WLAN Service:

ruckus(config-wlangrp)#
```

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 ID, 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'.
```

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 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.
```

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 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'.
> ```

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'.
> ```

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'.
```

access-ctrl

Enables access control policy.

Defaults

Disabled

Example

```
ruckus(config)# role role1
The Role entry 'role1' has been created.
ruckus(config-role)# access-ctrl
The command was executed successfully. To save the changes, type 'end' or 'exit'.
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
      Access Control Policy= Allowed
      Allow All OS Types:
        Mode= Allow all OS types to access
      VLAN = Any
      Rate Limiting Uplink = Disabled
      Rate Limiting Downlink = Disabled

ruckus(config-role)#
```

no access-ctrl

Disables access control policy.

no access-ctrl

dvc-type-allowed

To allow all or specify device type access, use the following command:

dvc-type-allowed [all|specify]

Example

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

specify-dvc-policy

To add the specified device policy into the role entry, use the following command:

specify-dvc-policy <WORD>

Example

```
ruckus(config-role)# specify-dvc-policy 0

ruckus(config-role)#
```

rate-limit uplink

Sets the rate limiting of uplink.

rate-limit uplink *NUMBER*

rate-limit uplink downlink

Sets the rate limiting of downlink.

rate-limit uplink *NUMBER* **downlink** *NUMBER*

no rate-limit

Sets rate limiting to Disable.

no rate-limit

apply-arc-policy

To configure an ARC policy with the specified name, use the following command:

apply-arc-policy*<WORD>*

Syntax Description

apply-arc-policy

Configures an Application Recognition and Control policy with the specified name.

WORD

Name of the ARC policy.

Defaults

None.

Example

```
ruckus(config-role)# apply-arc-policy Facebook
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-role)#
```

no apply-arc-policy

To disable ARC policy, use the following command:

no apply-arc-policy

Example

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

url-filtering

To configure URL Filtering with the specified name, use the following command:

url-filtering *WORD*

Defaults

None

Example

```
ruckus(config-role)# url-filtering filter1
Sorry, Please Enable 'Access Control Policy' firstly, then try again.
ruckus(config-role)#
```

no url-filtering

To disable URL filtering, use the following command:

no url-filtering

Defaults

None

Example

```
ruckus(config-role)# no url-filtering
Sorry, Please Enable 'Access Control Policy' firstly, then try again.
ruckus(config-role)#
```

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
      Access Control Policy= Disallowed

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

```
ruckus(config)# user johndoe1
The User entry 'johndoe1' 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 johndoe1
The User 'johndoe1' 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 (you must first set a password before exiting):

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 (you must first set a password before exiting):

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 *WORD*

Syntax Description

user-name

Set the name of a user

WORD

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 joeblow
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 12345678
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

The name of the role to be assigned to the user.

Defaults

Default

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= Joe
      Full Name= Joe Blow
      Password= ********
      Role= Default
```

```
ruckus(config-user)#
```

Configure Guest Access Commands

Use the guest-access commands to configure guest access services. To run these commands, you must first enter the **config-guest-access** context.

guest-access

To create/configure a Guest Access service and enter the config-guest-access context, use the following command:

guest-access *WORD*

Example

```
ruckus(config)# guest-access guestpolicy1
The Guest Access entry 'guestpolicy1' has been created.
ruckus(config-guest-access)#
```

no guest-access

To delete a Guest Access service, use the following command:

no guest-access

Example

```
ruckus(config)# no guest-access guest1
The Guest Access 'guest1' has been deleted.
ruckus(config)#
```

abort

To exit the config-guest-access context without saving changes, use the abort command.

abort

end

To save changes, and then exit the config-guest-access context, use the following command:

end

exit

To save changes, and then exit the config-guest-access context, use the following command:

exit

quit

To exit the config-guest-access context without saving changes, use the quit command.

quit

guest-access-force-https-redirection

Enables guest access force HTTPS redirection.

Syntax

guest-access-force-https-redirection

Command Default

Disabled

Examples

```
ruckus(config)# guest-access-force-https-redirection
The command was executed successfully.
ruckus(config)#
```

no guest-access-force-https-redirection

Disables guest access force HTTPS redirection.

Syntax

no guest-access-force-https-redirection

Command Default

Disabled.

Examples

```
ruckus(config)# no guest-access-force-https-redirection
The command was executed successfully.
ruckus(config)#
```

guest-access-guestpass-effective

To oset the guest pass effective date to begin from the creation time or from first use, use the following command:

guest-access-guestpass-effective [**now**|**first-use-expired <NUMBER>**]

Syntax Description

now

> Sets Effective from the creation time.

first-use-expired <NUMBER>

> Effective from first use, Expire new guest passes if not used within xx days.

Example

```
ruckus(config-guest-access)# guest-access-guestpass-effective first-use-expired 10
The command was executed successfully.
ruckus(config-guest-access)#
```

name

To set the name of the guest access policy, use the following command:

name *WORD*

self-service

To enable guest pass self-registration, use the following command:

self-service

no self-service

To disable guest pass self-registration, use the following command:

no self-service

guestpass-duration

To set the guest pass duration, use the following command:

guestpass-duration [**hour** | **day** | **week**] *NUMBER*

guestpass-reauth

To set the guest pass reauthorization timeout, use the following command:

guestpass-reauth [**hour** |**day** | **week**] *NUMBER*

no guestpass-reauth

To disable guest pass reauthorization timeout, use the following command:

no guestpass-reauth

guestpass-share-number

To set the limit on how many devices can share one guest pass, use the following command (valid values: [0, 10] and 0 means unlimited):

guestpass-share-number *NUMBER*

guestpass-sponsor

To enable guest pass sponsor approval, use the following command:

guestpass-sponsor

no guestpass-sponsor

To disable guest pass sponsor approval, use the following command:

no guestpass-sponsor

guestpass-sponsor-auth-server

Sets the authentication server to 'Local Database' or to a specified AAA server name, use the following command:

guestpass-sponsor-auth-server [**local** | **name** *WORD*]

guestpass-sponsor-number

To set the number of sponsors that can be used for this guest pass service (valid values: [1,5]), use the following command:

guestpass-sponsor-number *NUMBER*

guestpass-notification

To set the notification method for delivering guest passes, use the following command:

guestpass-notification *NUMBER*

Syntax Description

1

    Device Screen

2

    Mobile

3

    Emai

4

Mobile and Email

guestpass-terms-and-conditions

To enable and set the terms and conditions, use the following command:

guestpass-terms-and-conditions *WORD*

no guestpass-terms-and-conditions

To disable the terms and conditions, use the following command:

no guestpass-terms-and-conditions

onboarding

To configure onboarding portal options, use the following command:

onboarding [**key-and-zeroit**|**zeroit**]

Syntax Description

onboarding

Enable onboarding portal.

key-and-zeroit

Enables guest pass and zero-it activation.

zeroit

Enables zero-it activation only.

Defaults

Enabled, Guest Pass and Zero-IT.

Example

```
ruckus(config-guest-access)# onboarding key-and-zeroit
The command was executed successfully.
ruckus(config-guest-access)#
```

no onboarding

To disable the onboarding portal, use the following command:

no onboarding

no authentication

To disable guest access authentication, use the following command:

no authentication

Syntax Description

no authentication

        Disable guest access authentication

Defaults

Enabled.

Example

```
ruckus(config-guest-access)# no authentication
The command was executed successfully.
```

authentication guest-pass-and-social-login

To enable guest pass and social media login authentication for this guest access service, use the following command:

authentication guest-pass-and-social-login

Syntax Description

authentication guest-pass-and-social-login

        Enable guest pass and social media authentication.

Example

```
ruckus(config-guest-access)# authentication guest-pass-and-social-login
The command was executed successfully.
ruckus(config-guest-access)#
```

authentication only-social-login

To enable social media login only for this guest access service, use the following command:

authentication only-social-login

Syntax Description

authentication only-social-login

Enable social media authentication only.

Example

```
ruckus(config-guest-access)# authentication only-social-login
The command was executed successfully.
ruckus(config-guest-access)#
```

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 *WORD*

Syntax Description

term-of-use

Display Terms of Use

WORD

Display this text as content of Terms of Use on Guest Pass access page

Defaults

Disabled.

Example

```
ruckus(config-guest-access)# term-of-use test.guest
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

Disabled.

Example

```
ruckus(config-guest-access)# no term-of-use
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** *WORD*]

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 *WORD*

Redirect user to a different URL. Specify the URL in *WORD*.

Defaults

original

Example

```
ruckus(config-guest-access)# redirect url http://www.ruckuswireless.com
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)#
```

walled-garden

To set the walled garden URL, enter the following command:

walled-garden<INDEX><WORD>

Defaults

Disabled.

Example

```
ruckus(config-guest-access)# walled-garden 1 192.168.40.44
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-guest-access)#
```

no walled-garden

To delete the specified walled garden entry, enter the following command:

no walled-garden <INDEX>

Defaults

Disabled.

Example

```
ruckus(config-guest-access)# no walled-garden 1
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-guest-access)#
```

social-media-login

To set the social media login, use the following command:

social-media-login WORD

Syntax

<WORD>: Specify the social media login type:

- google <WORD> <WORD>: Sets the social media login to Google/Google+
- linkedin <WORD> <WORD>: Sets the social media login to LinkedIn
- microsoft <NUMBER> <WORD> <WORD>: Sets the social media login to Microsoft
- wechat <WORD> <WORD> <WORD> <WORD>: Sets the social media loging to WeChat.

Example

```
ruckus(config-guest-access)# social-media-login linkedin 1234456 test1
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-guest-access)#
```

social-media-login delete-social-media

To delete the social media, use the following command:

social-media-login delete-social-media <NUMBER>

Syntax Description

<NUMBER>

Delete the social media, google:3 linkdin:4 microsoft:5 wechat:6

Example

```
ruckus(config-guest-access)# social-media-login delete-social-media 3
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-guest-access)#
```

social-media-login google

To set the social media login to Google/Google+, use the following command:

social-media-login google NUMBER *WORD WORD*

NUMBER

Enter the redirection method 0:HTTP 1:HTTPS.

WORD

Enter the client ID.

WORD

Enter the client secret.

social-media-login hds

To set the Google host domain, use the following command:

social-media-login hds *<WORD>*

social-media-login no-hds

To clear the Google host domain, use the following command:

social-media-login no-hds

social-media-login linkedin

To set the social media login to LinkedIn, use the following command

social-media-login linkedin *WORD WORD*

social-media-login microsoft

To sets the social media login to Microsoft, use the following command:

social-media-login microsoft *NUMBERWORD WORD*

social-media-login wechat

To sets the social media login to WeChat, use the following command:

social-media-login wechat *WORDWORD WORDWORD*

social-media-login wechat force-follow

To set the WeChat social media WLAN to force follow , use the following command:

social-media-login wechat *WORDWORD WORDWORD* force-follow *WORD*

show

To display the guest access policy settings, use the following command:

show

Syntax Description

show
> Display the guest access settings

Example

```
ruckus(config-guest-access)# show
Guest Access:
  Name = guest1
  Onboarding Portal:
    Disabled
  Authentication:
    Mode = Use Guest Pass and Social login authentication
  Effective time:
    Countdown-by-issued = false
    Effective Period    = 7 Days
  Title = Welcome to Guest WiFi !
  Terms of Use:
    Status = Disabled
  Redirection:
    Mode = To the URL that the user intends to visit
  Self Service Registration:
    Status            = Disabled
  Wall Garden:

  Restricted Subnet Access:
      Rules:
        1:
           Description=
           Type= Deny
           Source Address= Any
           Destination Address= local
           Source Port= Any
           Destination Port= Any
           Protocol= Any
        2:
           Description=
           Type= Deny
           Source Address= Any
           Destination Address= 10.0.0.0/8
           Source Port= Any
           Destination Port= Any
           Protocol= Any
        3:
```

```
            Description=
            Type= Deny
            Source Address= Any
            Destination Address= 172.16.0.0/12
            Source Port= Any
            Destination Port= Any
            Protocol= Any
        4:
            Description=
            Type= Deny
            Source Address= Any
            Destination Address= 192.168.0.0/16
            Source Port= Any
            Destination Port= Any
            Protocol= Any

    Restricted IPv6 Access:
        Rules:
          1:
            Description=
            Type= Deny
            Source Address= Any
            Destination Address= local
            Source Port= Any
            Destination Port= Any
            Protocol= Any
            ICMPv6 Type= Any

   ruckus(config-guest-access)#
```

Configure Web Auth Settings

Use the following commands to configure web portal authentication settings.

web-portal-force-https-redirection

Enables web portal force HTTPS redirection.

Syntax

web-portal-force-https-redirection

Command Default

Disabled.

Examples

```
ruckus(config)# web-portal-force-https-redirection
The command was executed successfully.
ruckus(config)#
```

no web-portal-force-https-redirection

Disables web portal force HTTPS redirection.

Syntax

no web-portal-force-https-redirection

Command Default

Disabled.

Examples

```
ruckus(config)# no web-portal-force-https-redirection
The command was executed successfully.
ruckus(config)#
```

portal-auth-force-dns-server

Enables portal authentication WLAN (Hotspot Service, Guest Access and Web Authentication) force DNS server.

Syntax

portal-auth-force-dns-server <IP/IPv6-ADDR1 [IP/IPv6-ADDR2]>

Command Default

Disabled

Examples

```
ruckus(config)# portal-auth-force-dns-server 192.168.40.10
The command was executed successfully.
ruckus(config)#
```

no portal_auth-force-dns-server

Disable portal authentication WLAN (Hotspot Service, Guest Access and Web Authentication) force DNS server.

Syntax

no portal_auth-force-dns-server

Command Default

Disabled

Examples

```
ruckus(config)# no portal_auth-force-dns-server
The command was executed successfully.
ruckus(config)#
```

guest-access-auth-server

Sets the authentication server to 'Local Database' or to a specified AAA server.

Syntax

guest-access-auth-server { **local** | **name** *<WORD>*]

Command Default

None

Parameters

local

Sets the authentication server to 'Local Database'.

name <WORD>

Sets the authentication server to specified AAA server name.

Examples

```
ruckus(config)# guest-access-auth-server name radius1
The command was executed successfully.
ruckus(config)#
```

Configuring Guest Access Restriction Rules

Use the following commands to configure restricted access rules for a guest policy. To use these commands, you must enter the **config-guest-restrict-access** context from within the **config-guest-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

Example

```
ruckus(config-guest-access)# no restrict-access-order 4
The Restricted Subnet Access entry has been removed from the Guest Access.
ruckus(config-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.

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

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

Deny.

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

Deny.

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

Any.

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

Any.

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

Any.

Example

```
ruckus(config-guest-restrict-access)# protocol 69
The command was executed successfully.
```

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 no-mac-bypass

To disable MAC authentication bypass (no redirection), use the following command:

auth-server name *WORD* **no-mac-bypass**

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** [**mac** | **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)#
```

auth-server name mac-bypass mac-addr-format

To set MAC auth username and password to one of the following formats, use the following command:

auth-server name *WORD* **mac-bypass mac-addr-format** [**FORMAT**]

Syntax Description

auth-server name

Set an external authentication server for hotspot users

WORD

Authentication server name

mac-bypass

Enable MAC auth bypass

mac-addr-format

Enable MAC authentication bypass (no redirection) and use device MAC address as authentication password.

[**FORMAT**]

Set the MAC address format.

aabbccddeeff

Set the MAC address format to aabbccddeeff.

aa-bb-cc-dd-ee-ff

Set the MAC address format to aa-bb-cc-dd-ee-ff.

aa:bb:cc:dd:ee:ff

Set the MAC address format to aa:bb:cc:dd:ee:ff.

AABBCCDDEEFF

Set the MAC address format to AABBCCDDEEFF.

AA-BB-CC-DD-EE-FF

Set the MAC address format to AA-BB-CC-DD-EE-FF.

AA:BB:CC:DD:EE:FF

Set the MAC address format to AA:BB:CC:DD:EE:FF.

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 (on AP or across APs), use the following command:

client-isolation[**isolation-on-ap**| **isolation-across-ap**] [**enable** |**disable**]

Syntax Description

client-isolation

Enable client isolation.

isolation-on-ap

Enable client isolation per AP.

isolation-on-subnet

Enable spoof guarding and across AP client isolation using allowlist.

Defaults

Disabled

Example

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

allowlist

To apply a client isolation allowlist to this Hotspot, use the following command:

allowlist name *WORD*

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.
```

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.

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 NUMBER*

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 **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 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-consortiumNUMBER **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.

Example

```
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 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.

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 inner-EAP-mthd vndr-id *NUMBER*

Sets the vendor ID of the auth info.

auth-id exep-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
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

Example

```
ruckus(config)# mesh
ruckus(config-mesh)#
```

abort

To exit the config-mesh context without saving changes, use the abort command.

end

To save changes, and then exit the config-mesh context, use the end command.

exit

To save changes, and then exit the config-mesh context, use the exit command.

quit

To exit the config-mesh context without saving changes, use the quit command.

show

To display the current mesh settings, use the following command from within the *config-mesh* context:

show

Syntax Description

show

      Display the current mesh settings

Example

```
ruckus(config-mesh)# show
Mesh Settings:
  Mesh Status= Enabled
  Mesh Name(ESSID)= Mesh-951608000220
  Mesh Passphrase= bzj9Y0kEpkxOPzPXyKqLrJHZSAAnbtfaTm7Ebh6qps24PFPcc5MtCiijGGwFZBG
  Mesh Radio Option= 5G
  Mesh Uplink Selection Algorithm = default(static)
  Mesh Hop Detection:
    Status= Disabled
  Mesh Downlinks Detection:
    Status= Disabled
  Tx. Rate of Management Frame=  2Mbps
  Beacon Interval= 200ms
  Zero-Touch-Mesh status= Enabled
Zero Touch Mesh Pre-Approved Serial Number List:
serial number = 921802014959, approved = 0, time = 0, id = 1
serial number = 441e981cf0d0, approved = 0, time = 0, id = 2
serial number = 4f1e681cf3f0, approved = 0, time = 0, id = 3
serial number = c41e781bd7c0, approved = 0, time = 0, id = 4

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

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)#
```

mesh-uplink-selection static

Sets static on mesh uplinks, the default is static.

mesh-uplink selection static

Syntax Description

mesh-uplink-selection

Set the mesh uplink selection method.

static

Set mesh uplink selection to static.

Defaults

Static

Example

```
ruckus(config-mesh)# mesh-uplink-selection static
Nothing changed
ruckus(config-mesh)#
```

mesh-uplink-selection dynamic

Sets dynamic on mesh uplinks.

mesh-uplink selection dynamic

Syntax Description

mesh-uplink-selection

Set the mesh uplink selection method.

dynamic

Set mesh uplink selection to dynamic.

Defaults

Static

Example

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

mesh-radio-option

To set the mesh radio, use the following command:

mesh-radio-option <2.4G | 5G>

Options

2.4G: Sets mesh radio type to 2.4 GHz.

5G: Sets mesh radio type to 5 GHz.

Defaults

5G

Example

```
ruckus(config-mesh)# mesh-radio-option 5G
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-mesh)#
```

zero-touch-mesh

To enable zero touch mesh, use the following command:

zero-touch-mesh

Defaults

Disabled

Example

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

no zero-touch-mesh

To disable zero touch mesh, use the following command:

no zero-touch-mesh

Defaults

Disabled

Example

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

zt-mesh-serial

To add one or more zero-touch mesh pre-approved serial numbers, use the following command:

zt-mesh-serial[*<SERIAL_ 1> <SERIAL_ 2> <...> <SERIAL_n>*]

Syntax Description

zt-mesh-serial: Add zero-touch mesh pre-approved serial number.

<SERIAL_1>... : Serial number to be added to Zero Touch Mesh pre-approved list.

> **NOTE**
> The `zt-mesh-serial` command only submits these serial numbers to a system memory buffer. It does not save them to the pre-approved AP list. If you enter the `exit` or `end` command, these serial numbers will be saved to the pre-approved serial list and deleted from the system memory buffer. If you enter the `quit` or `abort` command, these serial numbers will been discarded and deleted from the system memory buffer.

Example

```
ruckus(config-mesh)# zt-mesh-serial 111122223333 222233334444 333344445555 444455556666
Add all serial numbers to zt-mesh pre-approved list submit ok!
ruckus(config-mesh)# end
Add 111122223333 to zt-mesh pre-approved list execute success!
Add 222233334444 to zt-mesh pre-approved list execute success!
Add 333344445555 to zt-mesh pre-approved list execute success!
Add 444455556666 to zt-mesh pre-approved list execute success!
Your changes have been saved.
ruckus(config)#
```

no zt-mesh-serial

To delete a zero-touch mesh pre-approved serial number, use the following command:

no zt-mesh-serial [*<SERIAL_1> <SERIAL_2> <...> <SERIAL_n>*]

Syntax Description

no zt-mesh-serial: Delete zero-touch mesh pre-approved serial number.

<SERIAL_1>... : Serial number to be removed from Zero Touch Mesh pre-approved list.

> **NOTE**
> The `no zt-mesh-serial` command only submits these serial numbers to a system memory buffer. It does not remove them from the pre-approved AP list. If you enter the `exit` or `end` command, these serial numbers will be removed from the pre-approved serial list and deleted from the system memory buffer. If you enter the `quit` or `abort` command, these serial numbers will been discarded and deleted from the system memory buffer.

Example

```
ruckus(config-mesh)# no zt-mesh-serial 111122223333 222233334444 333344445555 444455556666
Delete all serial numbers from zt-mesh pre-approved list submit ok!
ruckus(config-mesh)# end
Delete 111122223333 from zt-mesh pre-approved list execute success!
Delete 222233334444 from zt-mesh pre-approved list execute success!
Delete 333344445555 from zt-mesh pre-approved list execute success!
Delete 444455556666 from zt-mesh pre-approved list execute success!
Your changes have been saved.
ruckus(config)#
```

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

Defaults

Disabled

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

end

To save changes, and then exit the config-alarm context, use the following command:

end

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

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

Example

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

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'.
```

show

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

show

Example

```
ruckus(config-alarm)# show
Alarm:
  Status= Enabled
  Email Address= test@hotmail.com

ruckus(config-alarm)#
```

Configure Alarm-Event Settings

Use the alarm-event commands to configure which events will trigger ZoneDirector email alerts. Entering this command enters the **config-alarm-event** context.

alarm-event

To enter the config-alarm-event context and configure email alarm notifications for specific event types, use the following command:

alarm-event

event

To enable email alarm notifications for a specific alarm event, use the following command:

event *WORD*

Syntax Description

event all
> Enable email alarms for all event types

rogue-ap-detected
> Enable email notification when Rogue AP detected

rogue-device-detected
> Enable email notification when 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

user-blocked-ap-detected
> User blocked 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

radius-server-unreachable
> RADIUS 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

entitlement-download-fail

> Failure to download the Support Entitlement file from the RUCKUS Entitlement server

license-download-fail

> Failure to download the URL License file from the RUCKUS License Server.

test-alarm ap-lose-connection

> Test AP connection lost alarm event

show

> Show alarm settings

Defaults

All enabled

Example

```
ruckus(config)# alarm-event
ruckus(config-alarm-event)# event all
ruckus(config-alarm-event)# show
Alarm Events Notify By Email:
  MSG_rogue_AP_detected=                    enabled
  MSG_ad_hoc_network_detected=              enabled
  MSG_AP_lost=                              enabled
  MSG_SSID_spoofing_AP_detected=            enabled
  MSG_MAC_spoofing_AP_detected=             enabled
  MSG_admin_rogue_dhcp_server=              enabled
  MSG_admin_templic_expired=                enabled
  MSG_admin_templic_oneday=                 enabled
  MSG_same_network_spoofing_AP_detected=    enabled
  MSG_RADIUS_service_outage=                enabled
  MSG_AP_hardware_problem=                  enabled
  MSG_AP_no_mesh_uplink=                    enabled
  MSG_AP_keep_no_AC_cfg=                    enabled
  MSG_cltr_change_to_active=                enabled
  MSG_cltr_active_connected=                enabled
```

```
    MSG_cltr_standby_connected=                    enabled
    MSG_cltr_active_disconnected=                  enabled
    MSG_cltr_standby_disconnected=                 enabled
    MSG_user_blocked_AP_detected=                  enabled
    MSG_Entitlement_file_download_fail=            enabled
ruckus(config-alarm-event)#
```

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

user-blocked-ap-detected

User blocked 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

radius-server-unreachable

RADIUS 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

entitlement-download-fail

      Failure to download the Support Entitlement file from the RUCKUS Entitlement server

Example

```
ruckus(config-alarm-event)# no event aaa-server-unreachable
ruckus(config-alarm-event)# show
Alarm Events Notify By Email:
  MSG_rogue_AP_detected=                    enabled
  MSG_ad_hoc_network_detected=              enabled
  MSG_AP_lost=                              enabled
  MSG_SSID_spoofing_AP_detected=            enabled
  MSG_MAC_spoofing_AP_detected=             enabled
  MSG_admin_rogue_dhcp_server=              enabled
  MSG_admin_templic_expired=                enabled
  MSG_admin_templic_oneday=                 enabled
  MSG_same_network_spoofing_AP_detected=    enabled
  MSG_RADIUS_service_outage=                disabled
  MSG_AP_hardware_problem=                  enabled
  MSG_AP_no_mesh_uplink=                    enabled
  MSG_AP_keep_no_AC_cfg=                    enabled
  MSG_cltr_change_to_active=                enabled
  MSG_cltr_active_connected=                enabled
  MSG_cltr_standby_connected=               enabled
  MSG_cltr_active_disconnected=             enabled
  MSG_cltr_standby_disconnected=            enabled
  MSG_user_blocked_AP_detected=             enabled
  MSG_Entitlement_file_download_fail=       enabled

ruckus(config-alarm-event)#
```

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

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

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

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

Example

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

auto-channel-background-scanning

To configure auto channel background scanning settings, and enter the *ruckus(config-auto-channel-background-scanning)* context, use the following command:

auto-channel-background-scanning

Example

```
ruckus(config-services)# auto-channel-background-scanning
ruckus(config-auto-channel-background-scanning)#
```

radio-2.4

To enable auto channel background scanning on the 2.4 GHz radio, use the following command:

radio-2.4

Defaults

Enabled.

Example

```
ruckus(config-auto-channel-background-scanning)# radio-2.4
The command was executed successfully.
ruckus(config-auto-channel-background-scanning)#
```

no radio-2.4

To disable auto channel background scanning on the 2.4 GHz radio, use the following command:

no radio-2.4

Defaults

Enabled.

Example

```
ruckus(config-auto-channel-background-scanning)# no radio-2.4
The command was executed successfully.
ruckus(config-auto-channel-background-scanning)#
```

radio-5

To enable auto channel background scanning on the 5 GHz radio, use the following command:

radio-5

Defaults

Enabled.

Example

```
ruckus(config-auto-channel-background-scanning)# radio-5
The command was executed successfully.
ruckus(config-auto-channel-background-scanning)#
```

no radio-5

To disable auto channel background scanning on the 5 GHz radio, use the following command:

no radio-5

Defaults

Enabled.

Example

```
ruckus(config-auto-channel-background-scanning)# no radio-5
The command was executed successfully.
ruckus(config-auto-channel-background-scanning)#
```

off-period

To set the off period hours for auto channel background scanning, use the following command:

off-period <NUMBER><NUMBER>

Defaults

Disabled.

Example

```
ruckus(config-auto-channel-background-scanning)# off-period 23
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-auto-channel-background-scanning)#
```

no off-period

To disable the off period for auto channel background scanning, use the following command:

no off-period

Defaults

Disabled.

Example

```
ruckus(config-auto-channel-background-scanning)# no off-period
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-auto-channel-background-scanning)#
```

clients

To set the max number of associated clients per AP above which auto channel selection will not function, use the following command:

clients<NUMBER>

Defaults

Disabled.

Example

```
ruckus(config-auto-channel-background-scanning)# clients 100
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-auto-channel-background-scanning)#
```

interval

To set the auto channel selection interval (in minutes), use the following command:

interval <NUMBER>

Defaults

10 minutes.

Example

```
ruckus(config-auto-channel-background-scanning)# interval 10
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-auto-channel-background-scanning)#
```

threshold

To set threshold auto channel background scanning threshold (low|medium|high), use the following command:

threshold [*low* | *medium* | *high*]

Defaults

Medium.

Example

```
ruckus(config-auto-channel-background-scanning)# threshold low
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-auto-channel-background-scanning)#
```

simulate

To simulate auto channel selection with the current settings, use the following command:

simulate

Example

```
ruckus(config-auto-channel-background-scanning)# simulate
##############2.4G channel plan############
AP MAC            NB   Client  NB_Client  Rogue  Channel  Changed  New_Channel  New_NB  New_NB_Client
New_Rogue

##############5G channel plan##############
AP MAC            NB   Client  NB_Client  Rogue  Channel  Changed  New_Channel  New_NB  New_NB_Client
New_Rogue
d4:c1:9e:35:c9:40  0   1       0          0      40       No       NA           0       0                0

ruckus(config-auto-channel-background-scanning)#
```

deploy

To deploy auto channel background scanning with the current settings, use the following command:

deploy

Example

```
ruckus(config-auto-channel-background-scanning)# deploy
ruckus(config-auto-channel-background-scanning)#
```

show

To display auto channel background scanning settings, use the following command:

show

Example

```
ruckus(config-auto-channel-background-scanning)# show
      2.4GHZ radio status= Enabled
      5GHZ radio status= Enabled
      Off period hours = Disabled
      Interval = 1000 minutes
ruckus(config-auto-channel-background-scanning)#
```

auto-adjust-ap-power radio-2.4

To enable automatically adjusting AP 2.4 GHz radio power when interference is detected, use the following command:

auto-adjust-ap-power radio-2.4

Syntax Description

auto-adjust-ap-power

Enable the auto adjustment of the AP radio power.

radio-2.4

Enable the auto adjustment of the AP radio power on the 2.4 GHz radio.

Defaults

Disabled.

Example

```
ruckus(config-services)# auto-adjust-ap-power radio-2.4
The command was executed successfully.
```

no auto-adjust-ap-power radio-2.4

To disable automatically adjusting AP 2.4 GHz radio channel when interference is detected, use the following command:

no auto-adjust-ap-power radio-2.4

Syntax Description

no auto-adjust-ap-power

Disable the auto adjustment of the AP radio power.

radio-2.4

Disable the auto adjustment of the AP radio power on the 2.4 GHz radio.

Defaults

Disabled.

Example

```
ruckus(config-services)# no auto-adjust-ap-power radio-2.4
The command was executed successfully.
```

auto-adjust-ap-power radio-5

To enable automatically adjusting AP 5 GHz radio power when interference is detected, use the following command:

auto-adjust-ap-power radio-5

Syntax Description

auto-adjust-ap-power

> Enable the auto adjustment of the AP radio power.

radio-2.4

> Enable the auto adjustment of the AP radio power on the 5 GHz radio.

Defaults

Disabled.

Example

```
ruckus(config-services)# auto-adjust-ap-power radio-5
The command was executed successfully.
```

no auto-adjust-ap-power radio-5

To disable automatically adjusting AP 5 GHz radio channel when interference is detected, use the following command:

no auto-adjust-ap-power radio-5

Syntax Description

no auto-adjust-ap-power

> Disable the auto adjustment of the AP radio power.

radio-5

Disable the auto adjustment of the AP radio power on the 5 GHz radio.

Defaults

Enabled.

Example

```
ruckus(config-services)# no auto-adjust-ap-power radio-5
The command was executed successfully.
```

auto-adjust-ap-channel radio-2.4

To enable automatically adjusting the AP 2.4 GHz radio channel when interference is detected, use the following command:

auto-adjust-ap-channel radio-2.4

Syntax Description

auto-adjust-ap-channel

Enable the auto adjustment of the AP radio channel.

radio-2.4

Enable the auto adjustment of the AP radio channel on the 2.4 GHz radio.

Defaults

Enabled.

Example

```
ruckus(config-services)# auto-adjust-ap-channel radio-2.4
The command was executed successfully.
ruckus(config-services)#
```

no auto-adjust-ap-channel radio-2.4

To disable automatically adjusting the AP 2.4 GHz radio channel when interference is detected, use the following command:

no auto-adjust-ap-channel radio-2.4

Syntax Description

no auto-adjust-ap-channel

Disable the auto adjustment of the AP radio channel.

radio-2.4

Disable the auto adjustment of the AP radio channel on the 2.4 GHz radio.

Defaults

Enabled.

Example

```
ruckus(config-services)# no auto-adjust-ap-channel radio-2.4
The command was executed successfully.
ruckus(config-services)#
```

auto-adjust-ap-channel radio-5

To enable automatically adjusting the AP 5 GHz radio channel when interference is detected, use the following command:

auto-adjust-ap-channel radio-5

Syntax Description

auto-adjust-ap-channel

Enable the auto adjustment of the AP radio channel.

radio-5

Enable the auto adjustment of the AP radio channel on the 5 GHz radio.

Defaults

Enabled.

Example

```
ruckus(config-services)# auto-adjust-ap-channel radio-5
The command was executed successfully.
ruckus(config-services)#
```

no auto-adjust-ap-channel radio-5

To disable automatically adjusting the AP 5 GHz radio channel when interference is detected, use the following command:

no auto-adjust-ap-channel radio-5

Syntax Description

no auto-adjust-ap-channel

Disable the auto adjustment of the AP radio channel.

radio-5

Disable the auto adjustment of the AP radio channel on the 5 GHz radio.

Defaults

Enabled.

Example

```
ruckus(config-services)# no auto-adjust-ap-channel radio-5
The command was executed successfully.
ruckus(config-services)#
```

raps

To enable the Radar Avoidance Pre-Scanning (RAPS) feature on supported access points (SC-8800-S, 7782, 7781, etc.), use the following command:

raps

no raps

To disable the Radar Avoidance Pre-Scanning (RAPS) feature on supported access points (SC-8800-S, 7782, 7781, etc.), use the following command:

no raps

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

Enable ChannelFly channel management for 2.4G radios

```
ruckus(config-services)# channelfly radio-2.4 100
The command was executed successfully.
ruckus(config-services)#
```

Enable ChannelFly channel management for 5 G radios

```
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

Enables background scanning and configures the scan interval on an AP radio.

Syntax

background-scan {**radio-2.4-interval**|**radio-5-interval**|**radio-6-interval**} *number*

no background-scan {**radio-2.4-interval**|**radio-5-interval**|**radio-6-interval**} *number*

Command Default

By default, background scanning is enabled on all radios and the scan interval is set to 300 seconds.

Parameters

number

    Background scanning time interval, in seconds. Range is from 1 through 65535.

Syntax Description

Modes

Services configuration mode

Usage Guidelines

The *6 GHz* radio can be configured only on the tri-band APs.

The **no** form of the command removes the configured values for the radios.

Examples

The following example enables background scanning and sets the scan interval for the 2.4 GHz radio settings on an AP.

```
ruckus(config-services)# background-scan radio-2.4-interval 6
The command was executed successfully.
ruckus(config-services)#
```

History

Release version	Command history
200.16	This command was modified to include the 6 GHz radio setting.

background-scan low-threshold

To set the min threshold to switch channels for the 2.4 GHz radio, use the following command:

background-scan low-threshold <*NUMBER*>

Syntax Description

background-scan low-threshold
> Configure the low threshold for the radio.

NUMBER
> Set the minimum threshold value (0~2000).

Defaults

Disabled

Example

```
ruckus(config-services)# background-scan low-threshold 20
The command was executed successfully.
ruckus(config-services)#
```

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

Disabled

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

Disabled

Example

```
ruckus(config-services)# no aeroscout-detection
The command was executed successfully.
```

ekahau

To enable and set Ekahau Blink support with ERC IP and port, use the following command:

ekahau *ERC IP ERC Port*

Defaults

Disabled

Example

```
ruckus(config-services)# ekahau 10.10.10.1 500
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= 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
  RAPS= Enabled
  EKHAU settings:
    status= Enabled
    ERC IP= 10.10.10.1
    ERC port= 500
ruckus(config-services)#
```

no ekahau

To disable Ekahau Blink support, use the following command:

no ekahau

Defaults

Disabled

Example

```
ruckus(config-services)# no ekahau
The command was executed successfully.
ruckus(config-services)#
```

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

To enable multicast blocking for tunneled traffic, use the following command:

tun-block-mcast [**all**|**non-well-known**]

Syntax Description

all

Blocks all multicast traffic from network to tunnel.

non-well-known

Blocks non well-known multicast traffic from network to tunnel.

Defaults

Disabled

Example

```
ruckus(config-services)# tun-block-mcast all
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*

Syntax Description

tun-ip-ageing

Set ageing time for IP/IPv6 table.

NUMBER

Enter ageing time for IP/IPv6 table, ranging from 0 through 600 minutes.

Example

```
ruckus(config-services)# tun-ip-ageing
The command was executed successfully.
ruckus(config-services)# tun-ip-ageing 10
The command was executed successfully.
```

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**]

Example

```
ruckus(config-services)# no pif uplink-proc
The command was executed successfully.
ruckus(config-services)# no pif rate-limit
The command was executed successfully.
ruckus(config-services)#
```

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 following 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 *WORD*

Disable WIPS services

protect-excessive-wireless-request

Enables protecting the wireless network against excessive wireless requests

temp-block-auth-failed-client time *NUMBER*

Temporarily block wireless clients with repeated authentication failures for the specified time (in seconds)

rogue-report [**all**] | [**malicious** *ssid-spoofing* | **same-network** | **user-blocked** | **mac-spoofing**]

Enables report rogue devices in ZD event log.

all

Report all rogue devices.

malicious [*ssid-spoofing* | **same-network** | **user-blocked** | **mac-spoofing**]

Report particular malicious type.

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 30
The command was executed successfully.
ruckus(config-wips)# rogue-report all
The command was executed successfully.
ruckus(config-wips)# rogue-report malicious same-network
The command was executed successfully.
ruckus(config-wips)# rogue-dhcp-detection
The command was executed successfully.
ruckus(config-wips)# no rogue-dhcp-detection
The command was executed successfully.
ruckus(config-wips)# no rogue-report
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= 30 seconds
  Report rogue devices in ZD event log= Disabled
  Protect the network from malicious rogue access points= Disabled
  Rogue DHCP server detection= Disabled
ruckus(config-wips)#
```

Configure Email Server Commands

Use the email-server commands to configure email server settings. To run these commands, you must first enter the **config-email-server** context.

email-server

Use the following command to enter the **config-email-server** context and configure email server settings:

email-server

Syntax Description

help

Shows available commands.

history

Shows a list of previously run commands.

abort

Exits the config-email-server context without saving changes.

end

Saves changes, and the exits the config-email-server context.

exit

Saves changes, and the exits the config-email-server context.

quit

Exits the config-email-server context without saving changes.

enable

Enables the E-Mail server.

from *WORD*

Sets the E-Mail from for email server.

smtp-server-name *WORD*

Sets the smtp server name for email server.

smtp-server-port *NUMBER*

Sets the smtp server port for email server.

smtp-auth-name *WORD*

Sets the smtp authentication user name for email server.

smtp-auth-password *WORD*

Sets the smtp authentication password for email server.

smtp-wait-time

Sets the smtp server wait time (in seconds).

tls-smtp-encryption tls

Enables TLS of smtp encryption for email server.

tls-smtp-encryption starttls

Enables starttls in the TLS of smtp encryption for email server.

no enable

Disables the email server setting.

no tls-smtp-encryption tls

Disables TLS of smtp encryption for email server.

no tls-smtp-encryption starttls

Disables starttls in the TLS of smtp encryption for email server.

show

Shows email server settings.

Example

```
ruckus(config)# email-server
ruckus(config-email-server)# enable
ruckus(config-email-server)# from example@example.com
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-email-server)# smtp-server-name smtp.example.com
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-email-server)# smtp-server-port 587
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-email-server)# smtp-auth-name johndoe
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-email-server)# smtp-auth-password password
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-email-server)# tls-smtp-encryption tls
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-email-server)# tls-smtp-encryption starttls
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-email-server)# show
Email Server:
  Status= Enabled
  E-mail From = example@example.com
  SMTP Server Name= smtp.example.com
  SMTP Server Port= 587
  SMTP Authentication Username= johndoe
  SMTP Authentication Password= ********
  SMTP Encryption Options:
    TLS= Enabled
    STARTTLS= Enabled

ruckus(config-email-server)# end
The Email server settings have been updated.
Your changes have been saved.
ruckus(config)#
```

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-email-server)# from test1@gmail.com
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-email-server)#
```

enable

To enable the email server, use the following command:

enable

Example

```
ruckus(config-email-server)# enable
ruckus(config-email-server)#
```

no enable

To disale the email server, use the following command:

no enable

Example

```
ruckus(config-email-server)# no enable
ruckus(config-email-server)# show
Email Server:
  Status= Disabled

ruckus(config-email-server)#
```

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-email-server)# 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-email-server)# 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-email-server)# 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-email-server)# 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-email-server)# 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 email notifications, use the following command:

tls-smtp-encryption [**tls** | **starttls**]

Syntax Description

tls-smtp-encryption

Enable SMTP encryption of email notifications

tls

Enable TLS encryption for email notifications

starttls

Enable STARTTLS encryption for email notifications

Defaults

None.

Example

```
ruckus(config-email-server)# 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-email-server)# no tls-smtp-encryption tls
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

Configure SMS Server Commands

Use the sms-server commands to configure SMS server settings. To run these commands, you must first enter the **config-sms-server** context.

sms-server

Use the following command to enter the **config-sms-server** context and configure SMS server settings:

sms-server

Syntax Description

help

Shows available commands.

history

Shows a list of previously run commands.

abort

Exits the config-sms-server context without saving changes.

end

Saves changes, and the exits the config-sms-server context.

exit

Saves changes, and the exits the config-sms-server context.

quit

Exits the config-sms-server context without saving changes.

twilio

Configures SMS server settings for twilio. Enters ruckus(config-sms-server-twilio)#

clickatell

Configures SMS server settings for clickatell. Enters ruckus(config-sms-server-clickatell)#

account-sid *WORD*

Sets the account sid for twilio of sms server

auth-token *WORD*

Sets the auth token for twilio of sms server

from-phonenumber *WORD*

Sets the from phonenumber for twilio of sms server

country-code [*no-default-and-ask-user-to-input|default <country code default value> | default <country code default value> allow-change | default <country code default value> disallow-change*]

Sets the country code, default country code and whether to allow user input to change the country code from the default.

user-name *WORD*

Sets the user name for clickatell of sms server

password *WORD*

Sets the password for clickatell of sms server

api-id *WORD*

Sets the api id for clickatell of sms server

show

Displays the SMS server settings.

customized

Configures SMS server settings for customized server.Enters ruckus(config-sms-server-customized)#

url <WORD> <WORD>

Sets the URL for customized sms server

post <WORD>

Sets the post for customized sms server

Example

```
ruckus(config)# sms-server
ruckus(config-sms-server)# twilio
ruckus(config-sms-server-twilio)# account-sid abcdef123
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-sms-server-twilio)# auth-token word1234
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-sms-server-twilio)# country-code default +1 allow-change
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-sms-server-twilio)# from-phonenumber 6661231234
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-sms-server-twilio)# end
The SMS server settings have been updated.
Your changes have been saved.
ruckus(config-sms-server)# show
SMS Server:
  Server Type= twilio
    Account SID= abcdef123
    Auth Token= word1234
    From PhoneNumber= 6661231234
    Country Code= Use default +1 and allow user to change

ruckus(config-sms-server)# end
The SMS server settings have been updated.
Your changes have been saved.
ruckus(config)#
```

no sms-server

To disable SMS server settings, use the following command:

no sms-server

Example

```
ruckus(config)# no sms-server
The SMS server settings have been updated.
ruckus(config)#
```

country-code

Use the following command to configure SMS server country code settings:

country-code [*no-default-and-ask-user-to-input*|*default<WORD> + <NUMBER>* [*allow-change*|*disallow change*]]

Example

```
ruckus(config-sms-server-twilio)# country-code default +1 allow-change
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-sms-server-twilio)# end
The SMS server settings have been updated.
Your changes have been saved.
ruckus(config-sms-server)# show
SMS Server:
  Server Type= twilio
    Account SID= test123
    Auth Token= test123
    From PhoneNumber= 1112223344
    Country Code= Use default +1 and allow user to change

ruckus(config-sms-server)#
```

sns

To configure Short Notification Service settings and enter the *config-sns* context, use the following command:

sns

Syntax Description

abort	Exits the config-sns context without saving changes.
end	Saves changes, and then exits the config-sns context.
exit	Saves changes, and then exits the config-sns context.
quit	Exits the config-sns context without saving changes.
enable	Enables Short Notification Service.
no enable	Disables Short Notification Service.
show	Shows Short Notification Service settings.

Defaults

Enabled.

Example

```
ruckus(config)# sns
ruckus(config-sns)# enable
ruckus(config-sns)# show
Short Notification Service:
  Status= Enabled

ruckus(config-sns)# end
The Short Notification Service settings have been updated.
Your changes have been saved.
ruckus(config)#
```

Configure Station Rename Commands

Use the following commands to configure the renamed station list.

sta-rename

To create or modify the renamed station list, use the following commands:

Syntax Description

help	Shows available commands
history	Shows a list of previously run commands
no sta	Delete a renamed station
end	Save the current rule and quit
exit	Save the current rule and quit
abort	Discard the current rule and quit
quit	Discard the current rule and quit

Example

```
ruckus(config)# sta-rename
ruckus(config- sta-rename)# sta 6C:AA:B3:00:00:A0 my-iphone
ruckus(config- sta-rename)# end
Your changes have been saved. ruckus(config)# show sta-name Displays sta rename list:
MAC Address= 6C:AA:B3:00:00:A0
    rename= my-iphone


All sta rename number: 1.
ruckus(config)#
```

Configure Favorite Station Commands

Use the following commands to configure the favorite station list.

sta-favorite

To create or modify the favorite station list, use the following commands:

Syntax Description

help	Shows available commands
history	Shows a list of previously run commands
no sta	Delete a favorite station
sta <MAC>	Enable station favorite
end	Save the current rule and quit
exit	Save the current rule and quit
abort	Discard the current rule and quit
quit	Discard the current rule and quit

Example

```
ruckus(config)# sta-favorite
ruckus(config-sta-favorite)# sta aa:aa:aa:aa:aa:aa
ruckus(config-sta-favorite)# end
Your changes have been saved. ruckus(config)# show sta-favorite Displays sta favorite list:
MAC Address= aa:aa:aa:aa:aa:aa

All sta favorite number: 1.
ruckus(config)#
```

Configure mDNS (Bonjour) Commands

Use the following commands to configure mDNS (Bonjour Gateway) service.

mdnsproxy

Use the following command to enable mDNS proxy (Bonjour Gateway) service:

mdnsproxy [**zd** | **ap**]

no mdnsproxy

Use the following command to disable mDNS proxy (Bonjour Gateway) service:

no mdnsproxy [**zd** | **ap**]

mdnsproxyrule

Use the following command to create a new Bonjour Gateway rule or modify an existing rule, and enter the config-mdnsproxyrule context:

mdnsproxyrule *ID*

no mdnsproxyrule

Use the following command to delete a Bonjour Gateway rule:

no mdnsproxyrule *ID*

Configure Bonjour Policy

The following commands can be used from within the **config-bonjourpolicy** context to configure the Bonjour policy.

bonjour-policy

To create or edit a Bonjour policy, use the following command:

bonjour-policy *WORD*

Syntax Description

help

Shows available commands

history

Shows a list of previously run commands

no mdnsproxyrule

Delete mDNSproxy rule

mdnsproxyrule *ID*

Add/update mDNSproxy rules

note *NOTE*

Rule comments

end

Save the current rule and quit

exit

Save the current rule and quit

abort

Discard the current rule and quit

quit

Discard the current rule and quit

Example

```
ruckus(config)# bonjour-policy bonjour1
ruckus(config-bonjourpolicy)# note bonjourpolicy1
ruckus(config-bonjourpolicy)# end
Your changes have been saved.
ruckus(config)# show bonjour-policy
bonjour-policy:
  ID: 1
  Name: bonjour1
  Description: bonjourpolicy1
  rule:
ruckus(config)#
```

no bonjour-policy

To delete a Bonjour policy, use the following command:

no bonjour-policy *WORD*

Configure mDNS Proxy Rules

The following commands can be used from within the **config-mdnsproxyrule** context to configure the Bonjour Gateway bridge service rule.

Syntax Description

help

   Shows available commands

history

   Shows a list of previously run commands

service *Service-Name*

   Service name in ? list, or new bonjour rule

from-vlan *VLAN-From*

   VLAN from

to-vlan *VLAN-to*

   VLAN to

note *NOTE*

   Rule comments

show

   Show the current edited rule

end

   Save the current rule and quit

abort

   Discard the current rule and quit

quit

   Discard the current rule and quit

Example

```
ruckus(config-bonjourpolicy)# mdnsproxyrule 1
ruckus(config-policyrule)# service AirDisk
ruckus(config-policyrule)# from-vlan 220
ruckus(config-policyrule)# to-vlan 1
ruckus(config-policyrule)# note "share printer to vlan1"
ruckus(config-policyrule)# end
ruckus(config-bonjourpolicy)# end
ruckus(config)# show bonjour-policy
bonjour-policy:
  ID: 1
  Name: bonjour1
  Description: bonjourpolicy1
  rule:
   1:
    mdnsservice: AirDisk
    from_vlan:  br0.220
    to_vlan:        br0
    Notes:      share printer to vlan1
ruckus(config)#
```

Configure Bonjour Fencing Policy

To create a Bonjour Fencing policy and enter the **config-bonjourfencing** context, use the following command:

bonjour-fencing <*NAME*>

Syntax Description

bonjour-fencing

> Configure a Bonjour Fencing policy.

NAME

> Set the name of the fencing policy.

no <ID>	Delete fencing rules
show	Show the current edited bonjour fence
description	Sets the bonjour fence description.
fencerule <ID>	Add/Update fence rules
end	Save current rule and quit
exit	Save current rule and quit
abort	Discard current rule and quit
quit	Discard current rule and quit

Defaults

None.

Example

```
ruckus(config)# bonjour-fencing fence1
ruckus(config-bonjourfencing)#
  help                 Shows available commands.
  history              Shows a list of previously run commands.
  no <ID>              Delete fencing rules
  show                 Show the current edited bonjour fence
  description <WORD>   Sets the bonjour fence description.
  fencerule <ID>       Add/Update fence rules
  end                  Save current rule and quit
  exit                 Save current rule and quit
  abort                Discard current rule and quit
  quit                 Discard current rule and quit
ruckus(config-bonjourfencing)#
```

fencerule

To add or update fence rules, and enter the *config-fencerule* context, use the following command:

fencerule <*ID* >

Syntax Description

show	Show the current edited rule
source-type <TYPE>	Wired or wireless.
device-mac <MAC>	Device MAC.

anchor-ap <MAC>	Anchor AP MAC.
service <Service-Name>	List service names.
fencing-range <RANGE>	Fencing Range: Same AP or 1-Hop AP Neighbors.
description <WORD>	Fencing rule description.
end	Save current rule and quit
quit	Save current rule and quit

Example

```
ruckus(config-bonjourfencing)# fencerule 1
ruckus(config-fencerule)#
  help                  Shows available commands.
  history               Shows a list of previously run commands.
  show                  Show the current edited rule
  source-type <TYPE>    Wireless or Wired.
  device-mac <MAC>      Device MAC.
  anchor-ap <MAC>       Anchor AP MAC.
  service <Service-Name>
                        List service names.
  fencing-range <RANGE>
                        Fenceing Range: Same AP or 1-Hop AP Neighbors.
  description <WORD>    Fencing rule description.
  end                   Save current rule and quit
  exit                  Save current rule and quit
ruckus(config-fencerule)#
```

Configure Reportd Commands

Use the following commands to configure Reportd settings.

reportd

Use the following command to enter the **config-reportd** context and configure Reportd settings.

reportd

Syntax Description

help

Shows available commands

history

Shows a list of previously run commands

abort

Exits the config-reportd context without saving changes.

end

Save changes, and then exits the config-reportd context.

exit

Save changes, and then exits the config-reportd context.

quit

Exits the config-reportd context without saving changes.

enable

Enable Reportd settings.

disable

Disable Reportd settings.

wlan-url *WORD*

Set WLAN report URL.

ap-url *WORD*

Set AP report URL.

client-url *WORD*

Set client report URL.

system-url *WORD*

Set system report URL.

wlan-interval *NUMBER*

Sets WLAN report interval for Reportd in minutes.

ap-interval *NUMBER*

Sets AP report interval for Reportd in minutes.

client-interval *NUMBER*

Sets client report interval for Reportd in minutes.

system-interval *NUMBER*

Sets system report interval for Reportd in minutes.

wlan-compress *NUMBER*

Sets WLAN report compress-mode for Reportd.

ap-compress *NUMBER*

Sets AP report compress-mode for Reportd.

client-compress *NUMBER*

Sets client report compress-mode for Reportd.

system-compress *NUMBER*

Sets system report compress-mode for Reportd.

show

Displays Reportd settings.

Example

```
ruckus(config)# reportd
ruckus(config-reportd)# enable
The command was executed successfully. To save the changes, type 'end' or 'exit'
ruckus(config-reportd)# show
Reportd Settings:
  Reportd Status= Enabled
  WLAN report url=
  AP report url=
  Client report url=
  System report url=
  WLAN report interval= 15 min
  AP report interval= 15 min
  Client report interval= 15 min
  System report interval= 15 min
  WLAN compress mode= 0
```

```
AP compress mode= 0
Client compress mode= 0
System compress mode= 0
```

upload-debug

To configure upload debug file settings, use the following command:

upload-debugNUMBER

Syntax Description

abort	Exits the config-upload-debug context without saving changes.
end	Saves changes, and then exits the config-upload-debug context.
exit	Saves changes, and then exits the config-upload-debug context.
quit	Exits the config-upload-debug context without saving changes.
show	Shows upload debug file settings.
enable	Enables the upload debug file.
proto <tftp or ftp>	Sets the protocal for upload debug file.
host <WORD>	Sets the host for upload debug file.
port <NUMBER>	Sets the port for upload debug file.
ftp-user <WORD>	Sets the FTP username for upload debug file.
ftp-pass <WORD>	Sets the FTP password for upload debug file.

Defaults

Disabled.

Example

```
ruckus(config-upload-debug)#
  help                   Shows available commands.
  history                Shows a list of previously run commands.
  abort                  Exits the config-upload-debug context without saving changes.
  end                    Saves changes, and then exits the config-upload-debug context.
  exit                   Saves changes, and then exits the config-upload-debug context.
  quit                   Exits the config-upload-debug context without saving changes.
  show                   Shows upload debug file settings.
  enable                 Enables the upload debug file.
  proto <tftp or ftp>    Sets the protocal for upload debug file.
  host <WORD>            Sets the host for upload debug file.
  port <NUMBER>          Sets the port for upload debug file.
  ftp-user <WORD>        Sets the FTP username for upload debug file.
  ftp-pass <WORD>        Sets the FTP password for upload debug file.
ruckus(config-upload-debug)# enable
ruckus(config-upload-debug)# proto tftp
ruckus(config-upload-debug)# host 192.168.40.11
ruckus(config-upload-debug)# port 443
ruckus(config-upload-debug)# ftp-user user1
ruckus(config-upload-debug)# ftp-pass password1234
ruckus(config-upload-debug)# show
Upload Debug:
  Status= Enabled
  Protocal= TFTP
  Host = 192.168.40.11

ruckus(config-upload-debug)# end
The upload debug file settings have been updated.
Your changes have been saved.
ruckus(config)#
```

no upload-debug

Syntax

no upload-debug

Command Default

Disabled.

Examples

```
ruckus(config)# no upload-debug
The upload debug file settings have been updated.
ruckus(config)#
```

Using Debug Commands

Debug Commands Overview

This section describes the commands that you can use to debug Unleashed 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.

apfw_upgrade

To upgrade the controller's firmware, use the following command:

apfw_upgrade *<protocol>*://*server ip|server name/path/image name* [**-f**]

apfw_upgrade OPTIONS

Syntax Description

apfw_upgrade

Upgrade the AP'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)# apfw_upgrade
------------------------------------------------------------------------

Name: apfw_upgrade - AP Firmware Upgrade Tool (Ver.1.2)
Synopsis : apfw_upgrade tftp://<server ip|server name>/<path/image name>
------------------------------------------------------------------------
apfw_upgrade
ruckus(debug)#
```

restore

To restore the controller's configuration, use the following command:

Syntax

restore [**all** | **failover** | **policy**] *<IP-ADDR> <FILE-NAME>*

Parameters

restore

Restore controller's configuration.

all

Restore everything.

failover

Restore everything, except system name and IP address settings.

policy

Restore only WLAN settings, access control list, roles, and users.

policy

Restore only WLAN settings, access control list, roles, and users.

<IP-ADDR>

The IP address of the location of the backup file.

<FILE-NAME>

The file name of the backup file.

Examples

```
ruckus(debug)# restore all 192.168.0.9 backup.txt
 ** Checking if memory is sufficient**
 ** Downloading backup file **
 ** Verifying the backup file **
Invalid backup file
ruckus(debug)#
```

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.
```

wlaninfo

Configures and enables debugging of WLAN service settings. Enter wlaninfo without arguments to see all options.

wlaninfo *OPTIONS*

Syntax Description

wlaninfo

Enable logging of WLAN info

OPTIONS

Configure WLAN debug information options

Defaults

None.

Example

```
ruckus(debug)# wlaninfo -W -x
WLAN svc "Rhastah1" (id=1):
  WLAN ID = 0, ref_cnt = 7
  SSID = "Rhastah1" 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, DHCP relay = Disabled, vlan = 1, dvlan = Disabled,
bgscan = Enabled
  Proxy ARP = Disabled (IE:Disabled)
  wep key index = 0, wep key len = 0
  PAP message authenticator = Enabled, EAP-Failure = Disabled
  Device Policy = 0, Precedence = 1
  Smart Roam = Disabled Roam-factor = 1
  Hotspot2.0--WLAN = No (id=0)
  Num of VAP deployed: 6
    VAP: 04:4f:aa:0c:b1:0c, number of stations = 0
    VAP: 04:4f:aa:0c:b1:08, number of stations = 0
    VAP: c0:c5:20:3b:91:fc, number of stations = 1
    VAP: c0:c5:20:3b:91:f8, number of stations = 0
    VAP: c4:10:8a:1f:d1:fc, number of stations = 1
    VAP: c4:10:8a:1f:d1:f8, 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
    WPA PSK Pass Phrase:password
    WPA PSK Prev Pass Phrase:
    WPA PSK Pass Phrase (Hex):
        31306173 68613130
    WPA PSK:
        6aa94bac df5346ac ecc7d38f a14a6dbf
        7ba6f6f8 df2a4943 b23c9655 ac4f33de
    WPA Prev PSK:
        00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000
    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: disabled
  ToS Classification: enabled
  Dot1p Classification: disabled
  Multicast Filter: disabled
  Directed Threshold: 5
  Priority: Voice:0   Video:2   Data:4   Background:6
  Force DHCP: disabled   Timeout:10

*** Total WLAN Entries: 1 ***
ruckus(debug)#
```

show

To display parameters within the debug context, use the following command:

Syntax

show [**ap** | **station** | **logs** | **tls** | **remote-troubleshooting**]

Parameters

show

Display settings.

ap

Displays a list of all approved devices.

station

Displays a list of all connected stations (or clients).

logs

Displays a list of debug log components.

tls

Displays TLS version support.

remote-troubleshooting

Displays remote-troubleshooting.

Examples

```
ruckus(debug)# show tls
  TLS= Support TLS 1.0 and TLS 1.1
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)#
```

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

Example

```
ruckus(debug)# remote_ap_cli -A "get director"
---- Command 'rkscli -c "get director "' executed at c0:c5:20:3b:91:f0
------ ZoneDirector Info ------
Primary Controller   : n/a
Secondary Controller : n/a
DHCP Opt43 Code      : 3

The information of the most recent Zone Director:
  [1] 192.168.40.100

  AP is under management of ZoneDirector: 192.168.40.100 / c0:c5:20:18:97:c1,
  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] 192.168.40.100
```

```
     AP is under management of ZoneDirector: 192.168.40.100 / c0:c5:20:18:97:c1,
     Currently AP is in state: RUN
OK
---- Command Execution Summary:
          success: 2
          failure: 0
            total: 2
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)#
```

emfd-malloc-stats

Show uclibc malloc statistics.

Example

```
ruckus(debug)# emfd-malloc-stats
===== [pid=350] Sat Feb 15 15:58:42 2014
total bytes allocated           =    2691072
total bytes in use              =    2471920
total bytes freed               =     219152
total allocated mmap space      =     311296
number of free chunks           =         18
number of fastbin blocks        =          0
space in freed fastbin blocks   =          0
bin[ 1]: chunk_num=     1, list_len=     1, alloc_bytes=       4152, min_chunk[1]=       4152,
max_chunk[1]=      4152
bin[ 3]: chunk_num=     3, list_len=     3, alloc_bytes=         72, min_chunk[1]=         24,
max_chunk[1]=         24
```

```
bin[ 4]: chunk_num=      1, list_len=      1, alloc_bytes=          32, min_chunk[1]=          32,
max_chunk[1]=        32
bin[ 5]: chunk_num=      4, list_len=      4, alloc_bytes=         160, min_chunk[1]=          40,
max_chunk[1]=        40
bin[ 6]: chunk_num=      1, list_len=      1, alloc_bytes=          48, min_chunk[1]=          48,
max_chunk[1]=        48
bin[10]: chunk_num=      1, list_len=      1, alloc_bytes=          80, min_chunk[1]=          80,
max_chunk[1]=        80
bin[14]: chunk_num=      1, list_len=      1, alloc_bytes=         112, min_chunk[1]=         112,
max_chunk[1]=       112
bin[45]: chunk_num=      1, list_len=      1, alloc_bytes=        2928, min_chunk[1]=        2928,
max_chunk[1]=      2928
bin[49]: chunk_num=      1, list_len=      1, alloc_bytes=        5168, min_chunk[1]=        5168,
max_chunk[1]=      5168
bin[51]: chunk_num=      2, list_len=      2, alloc_bytes=       14952, min_chunk[1]=        7248,
max_chunk[2]=      7704
bin[52]: chunk_num=      1, list_len=      1, alloc_bytes=        8208, min_chunk[1]=        8208,
max_chunk[1]=      8208
ruckus(debug)#
```

save-config-as-default

To save the configuration to be restored upon reset to factory default settings, use the following command:

save-config-as-default

Defaults

Disabled.

Example

```
ruckus(debug)# save-config-as-default

The current configuration will be saved and will be restored when set-factory, are you sure(y/n):y

The configuration is saved successfully.
ruckus(debug)#
```

no save-config-as-default

To disable the saved configuration to be restored upon reset to factory default settings, use the following command:

no save-config-as-default

Defaults

Disabled.

Example

```
ruckus(debug)# no save-config-as-default

The saved configuration will be deleted, are you sure(y/n):y

The configuration is deleted successfully.
ruckus(debug)#
```

speedflex

To enable SpeedFlex on APs, use the following command:

speedflex

Defaults

Enabled.

Example

```
ruckus(debug)# speedflex
The System SpeedFlex has been enabled.
ruckus(debug)#
```

no speedflex

To disable SpeedFlex on APs, use the following command:

no speedflex

Defaults

Enabled.

Example

```
ruckus(debug)# no speedflex
The System SpeedFlex has been disabled.
ruckus(debug)#
```

support-tls

To configure the supported versions of TLS (ver. 1.0 or 1.1), use the following command:

Syntax

support-tls [**<VER>**]

Command Default

TLS 1.0 and TLS 1.1

Parameters

support-tls

Set TLS versions supported.

<VER>

TLS version 1.0, 1.1, or 1.0-1.1 (both).

Examples

```
ruckus(debug)# support-tls 1.0-1.1
Already support TLSv1.0 and TLSv1.1.
ruckus(debug)#
```

no support-tls

To disable support for TLS version 1.0 or 1.1, use the following command:

Syntax

no support-tls <VER>

Command Default

TLS version 1.0, 1.1 (both).

Parameters

<VER>

Select the TLS versions to disable.

Examples

```
ruckus(debug)# no support-tls 1.0
Are you sure you want to change whether support TLSv1.0, If yes, it will reboot Master.[Y/n]
ruckus(debug)#
```

ssh-icx

To configure the ICX CLI through the Unleashed CLI, use the following command:

Syntax

ssh-icx<USERNAME><ICX-IP>

Command Default

None

Examples

```
ruckus(debug)# ssh-icx admin 10.223.43.210

Host '10.223.43.210' is not in the trusted hosts file.
Do you want to continue connecting? (y/n) admin@10.223.43.210's password:
admin@10.223.43.210's password:

ruckus(debug)#
```

set-technical-support-wlan-mode

To configure the technical support WLAN deploy policy through the Unleashed CLI, use the following command:

Syntax

set-technical-support-wlan-mode<MODE><THRESHOLD>

set-technical-support-wlan-mode
> Set technical support WLAN policy to create support WLAN.

<MODE>
> Auto (Default): Technical support WLAN is created only if the number of APs (connected and disconnected) is less than or equal to threshold.
> Manual:Technical support WLAN is created regardless of the threshold parameter.
> Disable: Technical support WLAN creation is forbidden regardless of the threshold parameter.

<THRESHOLD>
> Default value is 5.

Command Default

None

Examples

```
ruckus(debug)# set-technical-support-wlan-mode Auto 10
ruckus(debug)#
```

security

To configure the security settings through the Unleashed CLI, use the following command:

Syntax

security [**medium** | **high**]

Command Default

None

Examples

```
ruckus(debug)# security
The command is either unrecognized or incomplete. To view a list of commands that you can run  from
this context, type '?' or 'help'.
ruckus(debug)# security high
ruckus(debug)# security medium
ruckus(debug)#
```

Show Commands

This section describes the show commands available within the debug context.

show ap

To display AP information for all APs, use the following command:

show ap

Example

```
ruckus(debug)# show ap
AP:
  ID:
    1:
      MAC Address= 44:1e:94:1b:f0:d0
      Model= r510
      Approved= Yes
      Device Name= RuckusAP
      Description=
      Location=
      GPS=
      CERT = Normal
      Bonjour-policy=
      Bonjour-fencing=
      Group Name= System Default
      Channel Range:
        A/N= 36,40,44,48,149,153,157,161 (Disallowed= )
        B/G/N= 1,2,3,4,5,6,7,8,9,10,11 (Disallowed= )
      Radio a/n:
        Channelization= Auto
        Channel= Auto
        WLAN Services enabled= Yes
        Tx. Power= Auto
        WLAN Group Name= Default
        Call Admission Control= OFF
        Protection Mode= Auto
      Radio b/g/n:
        Channelization= Auto
        Channel= Auto
        WLAN Services enabled= Yes
        Tx. Power= Auto
        WLAN Group Name= Default
        Call Admission Control= OFF
        Protection Mode= 2
      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= 192.168.0.10
        Netmask= 255.255.255.0
        Gateway= 192.168.0.1
        Primary DNS Server=
        Secondary DNS Server=

        Device IPv6 Settings= Keep AP's Setting
        IPv6 Type= Auto Configuration
        IPv6 Address= ::461e:98ff:fe1b:f0d0
        IPv6 Prefix Length= 64
        IPv6 Gateway=
        IPv6 Primary DNS Server=
        IPv6 Secondary DNS Server=
      Mesh:
        Mode= Use Parent Setting
```

```
    max hops= Use Parent Setting
  LLDP:
    Status = Use Parent Setting
  LAN Port:
    0:
      Interface= eth0
      Dot1x= None
      LogicalLink= Up
      PhysicalLink= Up 10Mbps full
      Label= 10/100/1000 PoE LAN1
    1:
      Interface= eth1
      Dot1x= None
      LogicalLink= Down
      PhysicalLink= Down
      Label= 10/100/1000 LAN2

2:
  MAC Address= d4:c2:9e:35:c9:50
  Model= r610
  Approved= Yes
  Device Name= RuckusAP
  Description=
  Location=
  GPS=
  CERT = Normal
  Bonjour-policy=
  Bonjour-fencing=
  Group Name= System Default
  Channel Range:
    A/N= 36,40,44,48,149,153,157,161 (Disallowed= )
    B/G/N= 1,2,3,4,5,6,7,8,9,10,11 (Disallowed= )
  Radio a/n:
    Channelization= Auto
    Channel= Auto
    WLAN Services enabled= Yes
    Tx. Power= Auto
    WLAN Group Name= Default
    Call Admission Control= OFF
    Protection Mode= Auto
  Radio b/g/n:
    Channelization= Auto
    Channel= Auto
    WLAN Services enabled= Yes
    Tx. Power= Auto
    WLAN Group Name= Default
    Call Admission Control= OFF
    Protection Mode= 2
  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= 192.168.0.3
    Netmask= 255.255.255.0
    Gateway= 192.168.0.1
    Primary DNS Server=
    Secondary DNS Server=

    Device IPv6 Settings= Keep AP's Setting
    IPv6 Type= Auto Configuration
    IPv6 Address= ::d6c1:9eff:fe35:c950
    IPv6 Prefix Length= 64
    IPv6 Gateway=
    IPv6 Primary DNS Server=
    IPv6 Secondary DNS Server=
  Mesh:
    Mode= Use Parent Setting
    max hops= Use Parent Setting
  LLDP:
    Status = Use Parent Setting
  LAN Port:
```

```
        0:
          Interface= eth0
          Dot1x= None
          LogicalLink= Up
          PhysicalLink= Up 1000Mbps full
          Label= 10/100/1000 PoE LAN1
        1:
          Interface= eth1
          Dot1x= None
          LogicalLink= Down
          PhysicalLink= Down
          Label= 10/100/1000 LAN2
      PoE Mode= Auto
      802.3af PoE Tx. chain= 2


ruckus(debug)#
```

show station

To display a list of all connected stations, use the following command:

show station

Example

```
ruckus(debug)# show station
Clients List:
  Client:
    MAC Address= c8:3a:6c:db:1a:3e
    User Name=
    IP Address= 192.168.0.5
    Access Point= d4:c2:9e:35:c9:40
    WLAN= Unleashed
    Channel= 1
    Signal (dB)= 90

  Client:
    MAC Address= 88:71:e6:a8:7a:d3
    User Name=
    IP Address= 192.168.0.7
    Access Point= d4:c2:9e:35:c9:40
    WLAN= Unleashed
    Channel= 40
    Signal (dB)= 63

  Client:
    MAC Address= 0c:91:61:88:d3:ca
    User Name=
    IP Address= 192.168.0.15
    Access Point= d4:c2:9e:35:c9:40
    WLAN= Unleashed
    Channel= 1
    Signal (dB)= 83

  Client:
    MAC Address= f0:04:8c:fb:73:38
    User Name=
    IP Address= 192.168.0.13
    Access Point= d4:c2:9e:35:c9:40
    WLAN= Unleashed
    Channel= 1
    Signal (dB)= 41

ruckus(debug)#
```

show logs

Displays a list of debug log components.

show logs

Example

```
ruckus(debug)# show logs
Debug Logs:
  All= Disabled
  Sys-mgmt= Disabled
  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
  Client-association= Disabled
  Debug logs of specified MAC address:
    Status= Disabled
ruckus(debug)#
```

show tls

To display the current TLS version support enabled, use the following command:

show tls

Example

```
ruckus(debug)# show tls
  TLS= Support TLS 1.0 and TLS 1.1
ruckus(debug)#
```

show save-config-as-default

To display the current save configuration, use the following command:

show save-config-as-default

Example

```
ruckus(debug)# show save-config-as-default
  Save-config-as-default= enable: true, Mon Apr 27 04:16:33 2020

ruckus(debug)#
```

show speedflex

To display SpeedFlex enabled status, use the following command:

show speedflex

Example

```
ruckus(debug)# show speedflex
  SpeedFlex= Enabled
ruckus(debug)#
```

show remote-troubleshooting

To display remote troubleshooting status, use the following command:

show remote-troubleshooting

Example

```
ruckus(debug)# show remote-troubleshooting
Ruckus CA troubleshooting is stopped!
The server addr is: None

ruckus(debug)#
```

ps

To display information about all processes that are running, use the following command:

ps

Example

```
ruckus(debug)# ps
  PID PPID USER     VSZ STAT COMMAND
    1    0 root    1184 S    init
    2    0 root       0 SW   [kthreadd]
    3    2 root       0 SW   [ksoftirqd/0]
    5    2 root       0 SW<  [kworker/0:0H]
    7    2 root       0 SW   [rcu_sched]
    8    2 root       0 SW   [rcu_bh]
    9    2 root       0 SW   [migration/0]
   10    2 root       0 SW   [watchdog/0]
   11    2 root       0 SW   [watchdog/1]
   12    2 root       0 SW   [migration/1]
   13    2 root       0 SW   [ksoftirqd/1]
   15    2 root       0 SW<  [kworker/1:0H]
   16    2 root       0 SW<  [khelper]
   17    2 root       0 SW   [irq/202-msmdata]
   18    2 root       0 SW<  [writeback]
   19    2 root       0 SW<  [bioset]
   20    2 root       0 SW<  [crypto]
   21    2 root       0 SW<  [kblockd]
   22    2 root       0 SW   [khubd]
   23    2 root       0 SW   [kswapd0]
   24    2 root       0 SW   [kworker/1:1]
   25    2 root       0 SW   [fsnotify_mark]
   26    2 root       0 SW   [kworker/u4:1]
   30    2 root       0 SW   [spi32766]
   39    2 root       0 SW<  [ipv6_addrconf]
   53    2 root       0 SW<  [deferwq]
   54    2 root       0 SW   [kworker/u4:2]
   55    2 root       0 SW   [ubi_bgt0d]
   62    1 root    1172 S    /bin/sh /usr/sbin/pad.sh
   65   62 root     720 S    /usr/sbin/pad
   68    1 root    5764 S <  /usr/sbin/rsmd start
   70    1 root    5740 S <  watchdog
   79    2 root       0 SW   [ubi_bgt1d]
```

```
   81     2 root          0 SW    [ubi_bgt2d]
   83     2 root          0 SW    [ubifs_bgt2_0]
  245    68 root       5808 S <   /usr/sbin/timer start
  261     2 root          0 SW<   [gmac_workqueue]
  262     2 root          0 SW<   [nss_data_plane_]
  263     2 root          0 SW<   [nss_freq_queue]
  264     2 root          0 SW<   [coredump_wait]
  329     1 root       8444 S     /usr/sbin/tcsd
  394     2 root          0 SW<   [alloc_task_wque]
  395     2 root          0 SW<   [alloc_task_wque]
  416     1 root       5900 S     eved
  444     1 root       1172 S     klogd -c 4
  498     1 root       2668 S     /usr/bin/mosquitto -c /tmp/mosquitto.conf
  501     1 root       2676 S     /usr/bin/matrix
  512     1 root       5764 S     rksmcast
  541     1 root       2792 S     /usr/sbin/dropbear -e /var/run/-login -I 900 -p
  588    68 root       5836 S <   /usr/sbin/rfwd start
  630     2 root          0 SW<   [uif-630]
  636     1 root      17960 S     /usr/sbin/apmgr -r start
  640     1 root       9712 S     /usr/sbin/election
  651  3147 root       1168 S     sleep 300
  652     1 root       5760 S     /usr/sbin/wrad
  659     1 root       6000 S     /usr/sbin/mdnsfence -p /tmp/mdnsfence.pid -b
  669     1 root       5736 S     hs20d
  699     1 root       5924 S     /usr/sbin/channelfly -i wifi0 -q
  710     1 root       2912 S     hostapd -B -g/var/run/hostapd-global -P/var/run
  714     1 root       5868 S     /usr/sbin/channelfly -i wifi1 -q
  716     1 root       6248 S     ztmd -s
  727     1 root       5996 S     /usr/sbin/rfmd -S
  729     1 root       7784 S     /usr/sbin/wipingd
  735     1 root       7400 S     cpd
  806     1 root       6176 S     /usr/sbin/avpd -D
  822     1 root      19300 S     /usr/sbin/uf_agent
  846     1 root       7116 S     /usr/sbin/statd -D
  853     1 root      33796 S     /usr/sbin/qm_dpi -D -n 1
  862     1 root       5744 S     dbdc
  867     1 root       5736 S     /usr/sbin/PoEMgr
  899     1 root       5740 S     rflow_radiod -b -m 2
  901     1 root       3032 S     /bin/wd_feeder
 1700     1 root       6652 S     /tmp/var/run/-login
 1705     1 root       1168 S     sleep 1000d
 1877     1 root       5720 S     snmpget -p /var/run/snmpget.pid1 -i 1
 1897     1 root       5724 S     snmpwalk -p /var/run/snmpwalk.pid1 -i 1
 1943  3269 root       1168 S     sleep 20
 1957  2488 root       1168 S     sleep 21
 1977    68 root          0 Z <   [rsmd_func]
 1978    68 root          0 Z <   [rsmd_func]
 1979    68 root          0 Z <   [rsmd_func]
 1980    68 root          0 Z <   [rsmd_func]
 1988    65 root        720 S     /usr/sbin/pad
 1989  1988 root       1172 S     sh -c /bin/ps -aux
 1990  1989 root       1176 R     /bin/ps -aux
 2032     1 root       1176 S     /bin/sh /bin/tsyslogd.sh
 2034  2032 root       3940 S     /bin/tsyslogd -r -h -n --rotate=21
 2036     1 root        980 S     /usr/sbin/in.tftpd -l -s /etc/airespider-images
 2088     1 root       1172 S     /bin/sh /bin/tacmon.sh
 2092  2088 root       3688 S     /bin/tacmon -i 30 -r 15
 2117     1 root       4384 S     /bin/emf_repo_flashsync monitor 15
 2118     1 root       3072 S     ttylogd
 2166     1 root       1124 S <   clusterD
 2167     1 root      26348 S     stamgr -d3 -t0
 2169     1 root      11996 S     apmgr_zd -r start
 2230     1 root       7168 S     upnpd
 2296     1 root      10432 S     getstatd
 2297     1 root      41668 S     emfd
 2298     1 root       5340 S N   sqlited
 2300     1 root      10488 S     rhttpc
 2488     1 root       1184 S     /bin/sh /usr/sbin/bonjour_mon.sh
 2882     1 root       1188 S     /sbin/udhcpc -b -i br0 --pidfile=/var/run/udhcp
 3145     1 root       2496 S     /usr/sbin/vsftpd /etc/vsftpd2.conf
 3147     1 root       1176 S     /bin/sh /bin/ftpdMon.sh
 3269     1 root       1176 S     /bin/sh /usr/sbin/pubnub_mon.sh un9418490011251
```

```
 3277  3269 root      8380 S    /usr/sbin/pubnubd un94184900112515729823628799
 3395     2 root         0 SW   [kworker/0:1]
 3450     1 root      2580 S    radsecproxy
 3474     1 root      1172 S    /sbin/udhcpp -i br0 --pidfile=/var/run/udhcpp.p
 3535     1 root     23988 S    /bin/webs
 3757     1 root      2376 S <  /usr/sbin/zapd
 3758     1 root      5876 S    lldpd -C d4:c1:9e:35:c9:40 -S Ruckus R610 Multi
 3763  3758 root      5888 S    lldpd -C d4:c1:9e:35:c9:40 -S Ruckus R610 Multi
 3845     1 root     14740 S    /usr/bin/stainfod
 4256     1 root      1416 S    mdnsd
 4301  2488 root       744 S    /usr/sbin/dns-sd -R Ruckus-Unleashed _ruckus-un
 5266    65 root       724 S    /usr/sbin/pad
 5290     1 root      3092 S    empty -f -L /tmp/empty/icx_01.tmp -i /tmp/empty
 5292  5290 root      2860 S    dbclient -y super@192.168.0.8
14982     2 root         0 SW   [kworker/1:2]
26640   541 root      2864 R    /usr/sbin/dropbear -e /var/run/-login -I 900 -p
26651 26640 root      1176 S    /bin/sh /var/run/-login
26652 26651 root      5588 S    /bin/login
26693 26652 root     10952 S    ruckus_cli2 -p VTCeYiFPy6&rw
27890     2 root         0 SW   [kworker/0:0]
ruckus(debug)#
```

show configuration_change_log

To display the configuration change log, use the following command:

show configuration_change_log

Example

```
ruckus(debug)# show configuration_change_log
 configuration changing log is on!

ruckus(debug)#
```

show-technical-support-wlan-mode

To display the technical support WLAN mode, use the following command:

show-technical-support-wlan-mode

Example

```
ruckus(debug)# show-technical-support-wlan-mode
 Technical support wlansvc mode:[Manual]
 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 the controller CLI. Configuration changes made through the AP CLI may be overwritten by controller settings if the AP is restarted or reconnects to the controller.

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

Example

```
ruckus(debug)# remote_ap_cli -A "get director"
---- Command 'rkscli -c "get director "' executed at c0:c5:20:3b:91:f0
------ ZoneDirector Info ------
Primary Controller   : n/a
Secondary Controller : n/a
DHCP Opt43 Code      : 3

The information of the most recent Zone Director:
  [1] 192.168.40.100

  AP is under management of ZoneDirector: 192.168.40.100 / c0:c5:20:18:97:c1,
  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] 192.168.40.100

  AP is under management of ZoneDirector: 192.168.40.100 / c0:c5:20:18:97:c1,
  Currently AP is in state: RUN
```

```
OK
---- Command Execution Summary:
        success: 2
        failure: 0
          total: 2
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

Usage Guidelines

Running this command can place considerable load on the system. If your ZoneDirector is already under load, running this command could potentially cause errors resulting in a reboot. In general, only use this command when working with RUCKUS support to troubleshoot an issue.

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
  Client-association= Enabled
  Debug logs of specified MAC address:
    Status= Disabled
ruckus(debug)#
```

no logs all

Disables debug logs of all debug components.

Syntax Description

no logs

Disable debug logs

all

Disable all log components

Example

```
ruckus(debug)# no logs all
The command was executed successfully.
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

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
  Client-association= Disabled
  Debug logs of specified MAC address:
    Status= Disabled
ruckus(debug)#
```

no logs comp sys-mgmt

Disables debug logs of system management components.

logs comp mesh

Enables debug logs of mesh components.

no logs comp mesh

Disables debug logs of mesh components.

logs comp web-auth

Enables debug logs of web authentication components.

no logs comp web-auth

Disables debug logs of web authentication components.

logs comp rf-mgmt

Enables debug logs of RF management components.

no logs comp rf-mgmt

Disables debug logs of RF management components.

logs comp radius

Enables debug logs of radius components.

no logs comp radius

Disables debug logs of radius components.

logs comp hotspot-srv

Enables debug logs of hotspot services components.

no logs comp hotspot-srv

Disables debug logs of hotspot services components.

logs comp aps

Enables debug logs of AP components.

no logs comp aps

Disables debug logs of access points components.

logs comp net-mgmt

Enables debug logs of network management components.

no logs comp net-mgmt

Disables debug logs of network management components.

logs comp 802.1x

Enables debug logs of 802.1x components.

no logs comp 802.1x

Disables debug logs of 802.1x components.

logs comp web-svr

Enables debug logs of web server components.

no logs comp web-svr

Disables debug logs of web server components.

logs comp 802.11

Enables debug logs of 802.11 components.

no logs comp 802.11

Disables debug logs of 802.11 components.

logs comp dvlan

Enables debug logs of dynamic VLAN components.

no logs comp dvlan

Disables debug logs of dynamic vlan components.

logs comp smart-redundancy

Enable Smart Redundancy component debug logs.

no logs comp smart-redundancy

Disable Smart Redundancy component debug logs.

logs comp bonjour-gateway

Enable Bonjour Gateway debug logs.

no logs comp bonjour-gateway

Disable Bonjour Gateway debug logs.

logs comp mdnsd

Enable bonjour mdnsd debug logs.

no logs comp mdnsd

Disable bonjour mdnsd debug logs.

logs comp client-association

Enable client association debug logs.

no logs comp client-association

Disable client association debug logs.

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

Example

```
ruckus(debug)# logs mac 04:4f:aa:0c:b1:00
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

Example

```
ruckus(debug)# no logs mac
The command was executed successfully.
ruckus(debug)#
```

logs winbind

To set the winbind log level (1-10), use the following command:

logs winbind<NUMBER>

Syntax Description

logs winbind

Set the winbind log level.

<NUMBER>

Choose the level of winbind debug logs.

Example

```
ruckus(debug)# logs winbind 3
killall: winbindd: no process killed
sh: winbindd: not found
ruckus(debug)#
```

logs level

To set the debug log level (1-10), use the following command:

logs level<NUMBER>

Syntax Description

logs level

Set the debug logs level.

<NUMBER>

Select a debug log level (1-10).

Example

```
ruckus(debug)# logs level 3
The command was executed successfully.
ruckus(debug)#
```

logs play

Starts displaying logs on console.

Syntax Description

logs

Enable debug logs

play

Start log play

Usage Guidelines

⚠️ **CAUTION**
Running this command can place considerable load on the system. If your ZoneDirector is already under load, running this command could potentially cause errors resulting in a reboot. In general, only use this command when working with RUCKUS support to troubleshoot an issue.

Example

```
ruckus(debug)# logs play
ruckus(debug)# [Feb 15 05:53:30][EMFD][debug]jobServiceFunc():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 play

Stops displaying logs on console.

Syntax Description

no logs

Disable debug logs

play

Stop log play

Example

```
rruckus(debug)# logs play
ruckus(debug)# [Feb 15 05:53:30][EMFD][debug]jobServiceFunc():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)#
```

support-tls

To set the TLS support version, use the following command:

support-tls<*VER*>

Defaults

1.0-1.1

Example

```
ruckus(debug)# support-tls 1.0-1.1
Already support TLSv1.0 and TLSv1.1.
ruckus(debug)#
```

no support-tls

To disable TLS support, use the following command:

no support-tls<*VER*>

configuration_change_log

To record all the configuration changes, use the following command:

configuration_change_log

Defaults

Disabled.

Example

```
ruckus(debug)# configuration_change_log
configuration changing log enabled!
ruckus(debug)# show configuration_change_log
configuration changing log is on!
ruckus(debug)#
```

no configuration_change_log

To disable the record of configuration changes, use the following command:

no configuration_change_log

Defaults

Disabled.

Example

```
ruckus(debug)# no save-config-as-default
configuration changing log disabled!
ruckus(debug)# show configuration_change_log
configuration changing log is off!
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)#
```

radius-stats-wlan

Show web-auth WLAN radius statistics bins.

radius-stats-authsvr

Show web-auth WLAN radius statistics bins.

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_coredupm

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)#
```

Accessing the AP-Mode CLI

Accessing the AP Mode CLI from the Unleashed CLI

To access the AP CLI from the Unleashed Master (controller) CLI, use the following command:

ap-mode

```
ruckus# ap-mode
You have all rights in this mode.
ruckus(ap-mode)#
```

Configure LTE Commands

The following CLI commands are provided to GET/SET the 3G/4G/LTE mobile configuration options for Unleashed LTE+Wi-Fi Access Points (Unleashed M510).

To use these CLI commands, you must enter the ap-mode CLI.

get lte

Use the following commands to display current LTE settings:

```
ruckus> en
ruckus# ap-mode
You have all rights in this mode.
ruckus(ap-mode)#
The following CLI commands are supported.
get lte-airplane-mode-state : get lte-airplane-mode-state
        Display LTE airplane mode state
get lte-default-eth-for-wan : get lte-default-eth-for-wan
        Display LTE default ethernet port for wan
get lte-failover-selection : get lte-failover-selection
        Display LTE failover selection info
get lte-gps-probe-interval : get lte-gps-probe-interval
        Display configured GPS probe interval time
get lte-imei : get lte-imei
        Display LTE IMEI info
get lte-internet-host : get lte-internet-host
    Display the remote host details configured for internet availability check
get lte-primary-wan-recovery-time : get lte-primary-wan-recovery-time
        Display primary wan recovery time
get lte-sim-apn : get lte-sim-apn {all|primary|secondary}
        Display LTE sim-apn info
get lte-sim-network-selection : get lte-sim-network-selection {all|primary|secondary}
        Display LTE sim-network-selection status
get lte-sim-password : get lte-sim-password {all|primary|secondary}
        Display LTE sim-password info
get lte-sim-pincode : get lte-sim-pincode {all|primary|secondary}
        Display LTE sim-pincode info
get lte-sim-roaming : get lte-sim-roaming {all|primary|secondary}
        Display LTE sim-roaming status

get lte-sim-selection : get lte-sim-selection
    Display LTE sim-selection info
get lte-sim-username : get lte-sim-username {all|primary|secondary}
    Display LTE sim-user-name info
get lte-state : get lte-state
```

```
    Display LTE state
get lte-statistics : get lte-statistics {all|primary|secondary}
    Display LTE status info
get lte-status : get lte-status
    Display LTE status
```

set lte

Use the following commands to configure LTE settings:

```
set lte-airplane-mode-state : set lte-airplane-mode-state {enable|disable}
    Set LTE airplane mode state
set lte-default-eth-for-wan : set lte-default-eth-for-wan {eth0|eth1}
    Set LTE default ethernet port for wan (It will be overwritten by WEB UI configuration)
set lte-failover-selection : set lte-failover-selection {ethernet-lte|lte-ethernet|ethernet|lte}
    Set LTE failover selection info (It will be overwritten by WEB UI configuration)
        ------------------------------
        ethernet-lte - primary ethernet, failover LTE
        lte-ethernet - primary LTE, failover ethernet
        ethernet - ethernet only
        lte - LTE only
        ------------------------------
set lte-gps-probe-interval : set lte-gps-probe-interval {seconds}
        Set how frequently to probe GPS coordinates
        min - 1 sec, max - 500000 sec
set lte-internet-host : set lte-internet-host {host_index} {status|addr|port} {value}
    Set the host address and TCP port number to confirm the internet availability
            {host_index} = numeric number, valid range = 0 to 4
     {status|addr|port} = specifies the purpose of {value}.
            {value} = {enable|disable} specific host if the previous attribute is 'status' (or)
            URL or IP address of remote host if the previous attribute is 'addr', max. allowed URL address
length = 255 (or)
            TCP port number if the previous attribute is 'port', valid port range = 0 to 65535.
Examples:
-> set lte-internet-host 0 addr www.google.com
    (Set www.google.com in 0'th index)
-> set lte-internet-host 0 port 443
    (Set port number 443 in 0'th index)
-> set lte-internet-host 0 status enable
    (Allow 0'th indexed host to be considered for internet reachability check)
-> set lte-internet-host 0 status disable
    (Don't use 0'th indexed host for internet reachability check)
Note:
The user must ensure the correctness and reliability of host URL/IP before the configuration.

set lte-primary-wan-recovery-time : set lte-primary-wan-recovery-time {seconds}
        Set primary wan recovery time (It will be overwritten by WEB UI configuration)
        min - 10 sec    max - 300 sec
set lte-reset : set lte-reset
    Reset LTE chip
    Note : Issue "set lte-state disable" before executing lte-reset
set lte-sim-apn : set lte-sim-apn {primary|secondary} {APN name} (It will be overwritten by WEB UI
configuration)
    max. allowed characters - 100
    allowed characters - A-Z, a-z, 0-9, (-)
set lte-sim-network-selection : set lte-sim-network-selection {primary|secondary} {lte|3g|auto}
set lte-sim-password : set lte-sim-password {primary|secondary} {Password}
    Omit the {Password} to disable/set to default
set lte-sim-pincode : set lte-sim-pincode {primary|secondary} {pincode}
    Omit the {pincode} to disable/set to default
set lte-sim-roaming : set lte-sim-roaming {primary|secondary} {enable|disable}

set lte-sim-selection : set lte-sim-selection {auto|primary|secondary}
        primary - SIM 0
        secondary - SIM 1
set lte-sim-username : set lte-sim-username {primary|secondary} {User name}
    Omit the {User name} to disable/set to default
set lte-state : set lte-state {enable|disable}
    Set LTE state
```

Configure OpenVPN Commands

The following CLI commands are provided to GET/SET the Open VPN configuration options for Unleashed.

To use these CLI commands, you must enter the ap-mode CLI.

get openvpn

Use the following commands to display current VPN settings:

```
ruckus> en
ruckus# ap-mode
You have all rights in this mode.
ruckus(ap-mode)#
The following CLI commands are supported.
get openvpn status
    Display the current openvpn status
get openvpn config
    Display the current openvpn configuration, including username and password
get openvpn statistics
    Display the statistics of the openvpn tunnel
```

set openvpn

Use the following commands to configure VPN settings:

```
set openvpn user {username} {password}
    Set the openvpn client username and password, which will be authenticated by the VPN server
set openvpn remote  {FQDN} {port}
    Set the remote openvpn server address and port
set openvpn service {enable|disable}
    Enable or disable the openvpn service
set openvpn config {options}
    Provide various openvpn configuration options
set openvpn config-remove {option keyword}
    Remove a specific option from the openvpn configuration
set openvpn cert {add|del} [local file name] {tftp|ftp|zd} [remote file name] {host|IP}
    Retrieve the openvpn root certificate to authenticate the openvpn server
set openvpn auth-server {enable|disable}
    Enable - the vpn client will authenticate the openvpn server by certificate before establishing the
connection
    Disable (default)
set openvpn persistent {true|false}
    True - the openvpn configuration file will be effective after set-factory
    False (default)
set openvpn clean
    Remove the openvpn configuration file and the user must re-configure openvpn after this command
set openvpn start
    Start the openvpn service
set openvpn stop
    Stop the openvpn service
```

Configure LACP Support Commands

The following CLI command is provided to GET the LACP status for a member AP on Unleashed.

To use these CLI commands, you must enter the ap-mode CLI.

get bond

Use the following command to display the LACP status on a member AP:

```
ruckus> en
ruckus# ap-mode
You have all rights in this mode.
ruckus(ap-mode)# get bond
LACP/Bonding is DISABLED.
OK
ruckus(ap-mode)# get bond
LACP/Bonding is ENABLED.
<bond0>
        Mode:           8023AD
        LACP-rate:      fast
        MII-Mon:        100 (ms)
        Xmit-Hash:      layer2+3
        Slaves:         2
        Slave-0:        eth0, ACTIVE, DOWN TOO LONG, link-fail-count: 0
        Slave-1:        eth1, ACTIVE, UP, link-fail-count: 0
OK
```

> **NOTE**
> The **get bond** command is supported for 11ax and Wave 2 APs.

> **NOTE**
> To enable or disable LACP on Master AP, use the **status-lacp [enable | disable]** command.

support

To execute AP CLI commands in the local AP, use the following command:

Syntax

support

Command Default

None

Examples

```
ruckus(ap-mode)# support
-----------RPM Config-------------
Enable       : 0
Rx-Cell      : 1
Interval     : 300 seconds
NBR Intvl    : 60 seconds
NBR Thr      : -85
Co-ch Thr    : -85
Use all ch   : 0
BGScan on    : 0
BGScan Intvl : 20 seconds
OnDemand Scan: 0
TxPwr Floor  : 6
RxSens Floor : 10
Syslog Lvl   : 3
sh: acsd_cli: not found
OK
ruckus(ap-mode)#
```