



Ruckus Wireless™ Unleashed™

Release 200.5 CLI Reference Guide

Part Number 800-71237-001 Rev B
Published October 2017

www.ruckuswireless.com

Copyright Notice and Proprietary Information

Copyright 2017. Ruckus Wireless, Inc. All rights reserved.

No part of this documentation may be used, reproduced, transmitted, or translated, in any form or by any means, electronic, mechanical, manual, optical, or otherwise, without prior written permission of Ruckus Wireless, Inc. ("Ruckus"), or as expressly provided by under license from Ruckus.

Destination Control Statement

Technical data contained in this publication may be subject to the export control laws of the United States of America. Disclosure to nationals of other countries contrary to United States law is prohibited. It is the reader's responsibility to determine the applicable regulations and to comply with them.

Disclaimer

THIS DOCUMENTATION AND ALL INFORMATION CONTAINED HEREIN ("MATERIAL") IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. RUCKUS AND ITS LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. RUCKUS RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

Limitation of Liability

IN NO EVENT SHALL RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIAL.

Trademarks

Ruckus Wireless, Ruckus, Bark Logo, BeamFlex, ChannelFly, Ruckus Pervasive Performance, SmartCell, ZoneFlex, Dynamic PSK, FlexMaster, MediaFlex, MetroFlex, Simply Better Wireless, SmartCast, SmartMesh, SmartSec, SpeedFlex, Unleashed, ZoneSwitch, and ZonePlanner are trademarks of Ruckus Wireless, Inc. in the United States and other countries. All other product or company names may be trademarks of their respective owners.

Contents

About This Guide	6
Document Conventions.....	7
Documentation Feedback.....	8
Online Training Resources	8
UnderstandingtheUnleashed Command Line Interface	9
Introduction.....	10
Accessing the Command Line Interface	10
Using the ? Command.....	14
Top-Level Commands	15
Using the Help Command.....	16
Viewing Current Configuration.....	17
Show Commands Overview	18
Show AAA Commands	18
Show DHCP Commands.....	21
Show Access Point Commands.....	22
Show AP Group Commands.....	29
Show System Configuration Commands.....	32
Show Performance Commands	34
Show System Information Commands.....	36
Show Ethernet Info Commands.....	37
Show Technical Support Commands	38
Show Management ACL Commands.....	40
Show Static Route Commands.....	41
Show WLAN Commands	42
Show WLAN Group Commands.....	44
Show L2 Access Control List Commands	46
Show Whitelist Commands	48
Show Whitelist Commands	49
Show L3 Access Control List Commands	50

Show Hotspot Commands.....	52
Show Guest Policy Commands	55
Show Role Commands.....	56
Show User Commands	59
ShowCurrentlyActiveClientsCommands.....	60
Show Mesh Commands.....	62
Show Dynamic PSK Commands	64
Show Dynamic Certificate Commands.....	65
Show Guest Pass Commands.....	65
Show Events and Activities Commands.....	66
Show Alarm Commands	68
Show License Commands.....	68
Show Session-Timeout Commands.....	69
Show RADIUS Statistics Commands.....	70
Show Load Balancing Commands.....	71

Configuring Master Settings.....97

Configuration Commands Overview	98
General Config Commands.....	98
Configure Context Show Commands.....	76
Configure AAA Server Commands.....	79
Configure DHCP Server Commands.....	82
Configure Admin Commands	84
Configure Access Points Commands	88
Configure AP Group Commands	111
Configure Hotspot Redirect Settings.....	121
ConfigureLayer2AccessControCommands.....	122
ConfigureLayer3AccessControCommands.....	129
ConfigureWhitelistCommands.....	140
Configure Band Balancing Commands.....	141
Configure Load Balancing Commands	143
Configure System Commands.....	148
ConfigureZero-ITSettings.....	176
Configure WLAN Settings Commands.....	178
ConfigureWLANGroupSettingsCommands.....	209
Configure Role Commands	215
Configure User Commands.....	228
Configure Guest Access Commands	234
Configure Hotspot Commands	244
Configure Mesh Commands.....	268

Configure Alarm Commands	275
ConfigureAlarm-EventSettings.....	475
Configure Services Commands.....	279
Configure WIPS Commands	291
Configure mDNS (Bonjour) Commands	294
Using Debug Commands.....	297
Debug Commands Overview.....	298
General Debug Commands	298
Show Commands	303
Accessing a Remote AP CLI.....	308
Working with Debug Logs and Log Settings.....	309
Remote Troubleshooting.....	316
AP Core Dump Collection	343
Script Execution	344
Example	348
Configure guest-access WLAN	348
Run AP CLI.....	352

About This Guide

The *Unleashed Release 200.5 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 Wireless 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 Wireless Support Web site at <https://support.ruckuswireless.com/documents>.

Document Conventions

The following two tables list the text and notice conventions that are used throughout this guide.

Table 1. Text conventions

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

Table 2. Notice conventions

Notice Type	Description
NOTE	Information that describes important features or instructions
CAUTION!	Information that alerts you to potential loss of data or potential damage to an application, system, or device
WARNING!	Information that alerts you to potential personal injury

Documentation Feedback

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

docs@ruckuswireless.com.

When contacting us, please include the following information:

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

For example:

- . Unleashed Release 200.5 CLI Reference Guide
- . Part number: 800-71237-001 Revision B
- . Page 88

Online Training Resources

To access a variety of online Ruckus Wireless training modules, including free introductory courses to wireless networking essentials, site surveys, and Ruckus Wireless products, visit the Ruckus Wireless Training Portal at:

<https://training.ruckuswireless.com>

Understanding the Unleashed Command Line Interface

1

In this chapter:

- Introduction
- Accessing the Command Line Interface
- Using the Help Command
- Top-Level Commands

Introduction

The Ruckus Wireless Unleashed Command Line Interface (CLI) is a software tool that enables you to configure and manage Unleashed, Ruckus Wireless's wireless LAN Master.

Using the command line interface, you can configure Master system settings, access points, wireless networks and client connection settings, or view current status information for each component of your Unleashed network. Each command performs a specific action for configuring device settings or returning information about the status of a specific device feature.

The Unleashed product is based on ZoneFlex, where the master AP is not only an AP, but also a controller, so Unleashed AP has two CLI systems. When you SSH to a member AP, you will go to the AP CLI system. When you SSH to the master AP, you will go to the Controller CLI system (which is like the ZoneDirector CLI system). This document describes the Unleashed controller CLI system.

Accessing the Command Line Interface

This section describes the requirements and the procedure for accessing the Unleashed CLI. The Unleashed CLI supports a maximum of 8 simultaneous SSH sessions, and maximum 4 sessions from the same IP address.

Requirements

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

- A computer that you want to designate as administrative computer
- A network connection to Unleashed
- A Telnet or SSH (secure shell) client program

Step 1: Connecting the Administrative Computer to Unleashed

The Unleashed Command Line Interface can be accessed using either an Ethernet or wireless connection.

Connect to Unleashed over Ethernet or Wi-Fi

- 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](#)"

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.

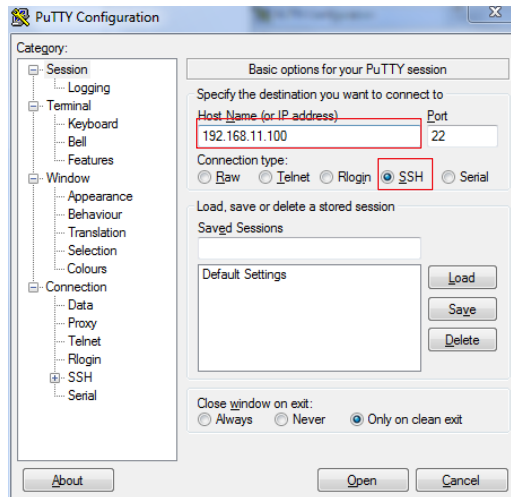
Using SSH

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 **SSH**.

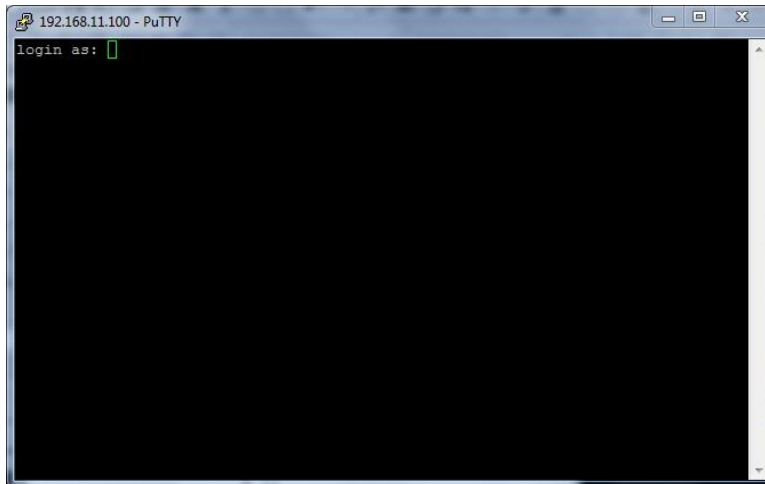
NOTE Telnet access is disabled by default for security reasons. SSH is the recommended access method and you will not be allowed to access the Unleashed CLI via Telnet unless you have specifically enabled Telnet access.

Figure 1. Selecting SSH as the connection type



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

Figure 2. 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.

- 1 At the `Please login` prompt, enter the Unleashed login name (default: **admin**), and then press `<Enter>`.
 - 2 At the `Password` prompt, enter the Unleashed login password (default: **admin**), and then press `<Enter>`. The Ruckus Wireless Unleashed CLI welcome message and the `ruckus>` prompt appears.
-

NOTE: Once the AP has been configured, use the login and password you configured to login to the CLI rather than the defaults (admin/admin).

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).

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

Using the ? Command

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

Example

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

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

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

<code>logs</code>	Contains commands that can be executed from within the context.
<code>no</code>	Contains commands that can be executed from within the context.
<code>remote-troubleshooting</code>	Troubleshooting commands group.
<code>script</code>	Manages system script for debug.

Top-Level Commands

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

<code>exit</code>	End the CLI session.
<code>help</code>	Show available commands.
<code>quit</code>	End the CLI session.
<code>history</code>	Show a list of previously run commands.
<code>disable</code>	Disable privileged commands.
<code>ping <IP-ADDR/ DOMAIN-NAME></code>	Send ICMP echo packets to an IP/IPv6 address or domain name.
<code>reboot</code>	Reboot the Master.
<code>shutdown</code>	Shut down Unleashed, to power on Unleashed again, press the power.
<code>set-factory</code>	Reset the Master to factory defaults.
<code>config</code>	Enter the config context.
<code>logo</code>	Configure Ruckus logo. Options are “logo nodog” and “logo default.”
<code>debug</code>	Enter the debug context.
<code>show</code>	Display system options and settings.
<code>reset</code>	Reset RADIUS statistics commands.

<code>session-timeout</code> <code><NUMBER></code>	Set the CLI session timeout.
<code>ap-mode</code>	Run AP CLI (set/get) in Master AP

Using the Help Command

To display all commands that the Ruckus Wireless 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.

Viewing Current Configuration

2

In this chapter:

- Show Commands Overview
- Show AAA Commands
- Show DHCP Commands
- Show Access Point Commands
- Show AP Group Commands
- Show System Configuration Commands
- Show System Information Commands
- Show WLAN Commands
- Show Hotspot Commands
- Show Guest Policy Commands
- Show User Commands
- Show Mesh Commands
- Show Guest Pass Commands
- Show Events and Activities Commands
- Show Alarm Commands

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 Master.

`show aaa all`

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

```
show aaa all
```

Syntax Description

<code>show</code>	Display information
<code>aaa</code>	Display AAA server information
<code>all</code>	All AAA servers

Defaults

None.

Example

```
ruckus# show aaa all
```

```
AAA:
```

```
ID:
```

```
1:
```

```
Name= Local Database
```

```
Type= Local
```

```
2:
```

```
Name= Guest Accounts  
Type= Guest
```

3:

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

4:

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

5:

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

show aaa name

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

```
show dhcp all
```

Syntax Description

<code>show</code>	Display information
<code>dhcp</code>	Display information about the specified DHCP server name
<code>all</code>	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 Master, 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 Master

Defaults

None.

Example

```
ruckus# show ap all
AP:
ID:
1:
MAC Address= 6c:aa:b3:3d:66:30
Model= r500
Approved= Yes
Device Name= R500-Unleashed
Device Role= Member
Description= ggk_unleahsed
Location= un
GPS=
CERT = Normal
Bonjour-policy=
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
    SpectraLink Compatibility= Disabled
Radio b/g/n:
    Channelization= Auto
    Channel= Auto
    WLAN Services enabled= Yes
    Tx. Power= Auto
    WLAN Group Name= Default
    Call Admission Control= OFF
    SpectraLink Compatibility= Disabled
Override global ap-model port configuration= No
Network Setting:
    Protocol mode= IPv4-Only
    Device IP Settings= Manual
    IP Address= 172.18.151.1
    Netmask= 255.255.255.0
```

```
Gateway=
Primary DNS Server= 172.18.100.35
Secondary DNS Server= 172.18.100.45
Mesh:
  Status= Enabled
  Mode= Auto
  max hops= unlimited
Uplink:
  Status= Smart
LLDP:
  Status = Enabled
  Interval = 30
  HoldTime = 120
  Mgmt = Enabled
Ports:
  Send out LLDP packet on eth0 = Enabled
  Send out LLDP packet on eth1 = Enabled
Venue Name List:
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

  2:
    MAC Address= 94:f6:65:3c:cf:a0
    Model= r500
    Approved= Yes
    Device Name= RuckusAP
    Device Role= Master
    Description=
    Location=
    GPS=
    CERT = Normal
    Bonjour-policy=
    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
SpectraLink Compatibility= Disabled
Radio b/g/n:
Channelization= Auto
Channel= Auto
WLAN Services enabled= Yes
Tx. Power= Auto
WLAN Group Name= Default
Call Admission Control= OFF
SpectraLink Compatibility= Disabled
Override global ap-model port configuration= No
Network Setting:
Protocol mode= IPv4-Only
Device IP Settings= DHCP
IP Address= 172.18.151.2
Netmask= 255.255.255.0
Gateway= 0.0.0.0
Primary DNS Server= 172.18.100.35
Secondary DNS Server= 172.18.100.45
Mesh:
Mode= Use Parent Setting
max hops= Use Parent Setting
LLDP:
Status = Use Parent Setting
Venue Name List:
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
```

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 "R500-Unleashed"
AP:
ID:
1:
MAC Address= 6c:aa:b3:3d:66:30
Model= r500
Approved= Yes
Device Name= R500-Unleashed
Device Role= Member
Description= ggk_unleashed
Location= un
GPS=
CERT = Normal
Bonjour-policy=
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
    SpectraLink Compatibility= Disabled
Radio b/g/n:
    Channelization= Auto
    Channel= Auto
    WLAN Services enabled= Yes
    Tx. Power= Auto
    WLAN Group Name= Default
    Call Admission Control= OFF
    SpectraLink Compatibility= Disabled
Override global ap-model port configuration= No
Network Setting:
    Protocol mode= IPv4-Only
    Device IP Settings= Manual
```

```
IP Address= 172.18.151.1
Netmask= 255.255.255.0
Gateway=
Primary DNS Server= 172.18.100.35
Secondary DNS Server= 172.18.100.45
Mesh:
  Status= Enabled
  Mode= Auto
  max hops= unlimited
Uplink:
  Status= Smart
LLDP:
  Status = Enabled
  Interval = 30
  HoldTime = 120
  Mgmt = Enabled
Ports:
  Send out LLDP packet on eth0 = Enabled
  Send out LLDP packet on eth1 = Enabled
Venue Name List:
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
```

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 6c:aa:b3:3d:66:30
AP:
ID:
1:
MAC Address= 6c:aa:b3:3d:66:30
Model= r500
Approved= Yes
Device Name= R500-Unleashed
Device Role= Member
Description= ggk_unleahsed
Location= un
GPS=
CERT = Normal
Bonjour-policy=
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
    SpectraLink Compatibility= Disabled
Radio b/g/n:
    Channelization= Auto
    Channel= Auto
    WLAN Services enabled= Yes
    Tx. Power= Auto
    WLAN Group Name= Default
    Call Admission Control= OFF
    SpectraLink Compatibility= Disabled
Override global ap-model port configuration= No
Network Setting:
    Protocol mode= IPv4-Only
    Device IP Settings= Manual
    IP Address= 172.18.151.1
    Netmask= 255.255.255.0
    Gateway=
    Primary DNS Server= 172.18.100.35
    Secondary DNS Server= 172.18.100.45
Mesh:
    Status= Enabled
    Mode= Auto
    max hops= unlimited
Uplink:
    Status= Smart
```



```
LLDP:
  Status = Enabled
  Interval = 30
  HoldTime = 120
  Mgmt = Enabled
Ports:
  Send out LLDP packet on eth0 = Enabled
  Send out LLDP packet on eth1 = Enabled
Venue Name List:
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 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 (now only default AP group: **System Default is supported**), 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

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
  MLD Query v1= Disabled
  MLD Query v2= Disabled
  IGMP Query v2= Disabled
  IGMP Query v3= Disabled
  Location Base Service:
    State = Disabled
    Location Server = NA
  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= 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
    Wlan Service= Enabled
  Network Setting:
    Protocol mode= IPv4 and IPv6
  Mesh:
    max hops= unlimited
    Mode= Auto
    Turn off channfly setting:
```

```
state= Disabled
if AP's uptime is more than 30 minutes will turn
off AP's ChannelFly
Members:
MAC= 6c:aa:b3:3d:66:30
MAC= 94:f6:65:3c:cf:a0

ruckus#
```

Show System Configuration Commands

Use the `show config` commands to display the Master'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

<code>show</code>	Display information
<code>config</code>	Display system configuration settings

Defaults

None.

Example

```
ruckus# show config
Protocol Mode= IPv4-Only
Device IP Address:
Mode= Manual
IP Address= 172.18.151.2
Netmask= 255.255.255.0
Gateway Address= 172.18.151.254
Primary DNS= 172.18.100.35
```

Secondary DNS= 172.18.100.45

Country Code:

Code= United States

Identity:

Name= Ruckus-Unleashed-ggk

Session Statistics:

Enable= false

Limited Unauthorized Session= true

NTP:

Status= Enabled

Address= ntp.ruckuswireless.com

Timezone= GMT

Log:

Status= Disabled

Address=

Facility=

Priority=

AP Facility=

AP Priority=

event log level= 1

Telnet Server:

Status= Disabled

FTP Server:

Status= Enabled

Anonymous Status= Disabled

FlexMaster:

Status= Disabled

Address=

Interval= 15

AAA:

ID:

1:

Name= Local Database

Type= Local

Show Performance Commands

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

show performance

Use the following command to display performance details:

```
show performance
```

show performance ap-radio2-4

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

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

Syntax Description

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

Defaults

None.

Example

```
ruckus# show performance ap-radio2-4 mac c4:10:8a:1f:d1:f0
AP performance:
  1:
    Radio b/g/n:
    MAC Address= c4:10:8a:1f:d1:f0
    Estimated Capacity= 9930
    Downlink= 67
    Uplink= 0
    RF pollution= 11
    Associated clients= 1
    Other APs= 0
ruckus#
```

show performance ap-radio5

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

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

Syntax Description

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

Defaults

None.

Example

```
ruckus# show performance ap-radio5 mac c4:10:8a:1f:d1:f0
```

AP performance:

1:

Radio a/n:

MAC Address= c4:10:8a:1f:d1:f0

Estimated Capacity= 20891

Downlink= 77

Uplink= 2

RF pollution= 3

Associated clients= 1

Other APs= 0

```
ruckus#
```

show performance station

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

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

Syntax Description

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

Defaults

None.

Example

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

Show System Information Commands

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

show sysinfo

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

```
show sysinfo
```

Syntax Description

<code>show</code>	Display information
<code>sysinfo</code>	Display an overview of various system statuses

Defaults

None.

Example

```
ruckus# show sysinfo
System Overview:
    Name= Ruckus-Unleashed-ggk
    IP Address= 172.18.151.2
    MAC Address= 94:F6:65:3C:CF:A0
    Uptime= 4d 0h 18m
    Model= R500
    Licensed APs= 25
    Serial Number= 161594206569
    Version= 200.3.9.13 build 14866331
```

Devices Overview:

```
    Number of APs= 3
```



```
Number of Client Devices= 2  
Number of Rogue Devices= 15
```

Usage Summary:

```
Usage of 1 hr:  
  Max. Concurrent Users= 2  
  Bytes Transmitted= 45.87M  
  Number of Rogue Devices= 15  
Usage of 24 hr:  
  Max. Concurrent Users= 3  
  Bytes Transmitted= 5.90G  
  Number of Rogue Devices= 50
```

Memory Utilization:

```
Used Bytes= 61009920  
Used Percentage= 47%  
Free Bytes= 67158016  
Free Percentage= 53%
```

```
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= 94:f6:65:3c:cf:a3
Physical Link= up
Speed= 1000Mbps
Port 1:
Interface= eth1
MAC Address= 94:f6:65:3c:cf:a4

Physical Link= up
Speed= 1000Mbps
```

```
ruckus#
```

Show Technical Support Commands

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

show techsupport

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

```
show techsupport
```

Syntax Description

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

Defaults

None.

Example

```
ruckus# show techsupport
ruckus# show techsupport
System Overview:
  Name= Ruckus-Unleashed-ggk
  IP Address= 172.18.151.2
  MAC Address= 94:F6:65:3C:CF:A0
  Uptime= 15d 18h 44m
```

```
Model= R500
Licensed APs= 25
Serial Number= 161594206569
Version= 200.3.9.13 build 14866331
Devices Overview:
  Number of APs= 2
  Number of Client Devices= 3
  Number of Rogue Devices= 798
Usage Summary:
  Usage of 1 hr:
    Max. Concurrent Users= 2
    Bytes Transmitted= 76.66M
    Number of Rogue Devices= 0
  Usage of 24 hr:
    Max. Concurrent Users= 0
    Bytes Transmitted= 2.24G
    Number of Rogue Devices= 0
Memory Utilization:
  Used Bytes= 95956992
  Used Percentage= 74%
  Free Bytes= 32210944
  Free Percentage= 26%
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=
Country Code:
  Code= United States
Identity:
  Name= Ruckus-Unleashed-ggk
...
...
ruckus#
```

Show Management ACL Commands

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

show mgmt-acl all

To display all management ACLs that have been configured on the Master, 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>
```

Syntax Description

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

Defaults

None.

Example

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

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

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

ruckus#
```

Show Static Route Commands

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

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>
```

Syntax Description

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

Defaults

None.

Example

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

```
ruckus#
```

Show WLAN Commands

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

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(config)# show wlan all
WLAN Service:
  ID:
  1:
    NAME = Ruckus-Wireless 1-ggk
    Tx. Rate of Management Frame (2.4GHz) = 2.0Mbps
    Tx. Rate of Management Frame (5GHz) = 6.0Mbps
    Beacon Interval = 100ms
    SSID = Ruckus-Wireless 1-ggk
    Description = Ruckus-Wireless 1-ggk
    Type = Standard Usage
    Authentication = open
    Encryption = open
    Algorithm = aes
    Passphrase = 88888888
    FT Roaming = Disabled
    802.11k Neighbor report = Disabled
```

```
Web Authentication = Disabled
Authentication Server = Disabled
Called-Station-Id type = wlan-bssid
Tunnel Mode = Disabled
Background Scanning = Enabled
Max. Clients = 100
Isolation per AP = Disabled
Isolation across AP = Disabled
Zero-IT Activation = Enabled
Priority = High

Load Balancing = Enabled
Band Balancing = Enabled
Dynamic PSK = Enabled
Dynamic PSK Passphrase Length = 62
Dynamic PSK Type = friendly
Dynamic PSK Expire Time = one-day
Dynamic PSK Validity Period = first-use
Limit Dynamic PSK = Disabled
Rate Limiting Uplink = Disabled
Rate Limiting Downlink = Disabled
Auto-Proxy configuration:
    Status = Disabled
Inactivity Timeout:
    Status = Enabled
    Timeout = 5 Minutes
VLAN-ID = 1
Dynamic VLAN = Disabled
Closed System = Disabled
Https Redirection = Disabled
OFDM-Only State = Disabled
Multicast Filter State = Disabled
802.11d State = Enabled
Force DHCP State = Disabled
Force DHCP Timeout = 10
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 = Default
Proxy ARP = Disabled
Device Policy = No ACLS
Vlan Pool = No Pools
Role based Access Control Policy = Disabled
SmartRoam = Disabled  Roam-factor = 1
White List = No ACLS
Application Visibility = enabled
Apply Policy Group = No_Denys
Wlan Bind = all
```

```
ruckus(config)#
```

Show WLAN Group Commands

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

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=

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

<code>show</code>	Display information
<code>l2acl</code>	Display L2 ACL information
<code>all</code>	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 Whitelist Commands

Use the `show whitelist` commands to display client isolation whitelists that have been added to the controller.

show whitelist all

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

```
show whitelist all
```

Syntax Description

<code>show</code>	Display information
<code>whitelist</code>	Display whitelist information
<code>all</code>	All whitelists

Defaults

None.

Example

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

ruckus#
```

Show Whitelist Commands

Use the `show whitelist` commands to display client isolation whitelists that have been added to the Master.

show whitelist all

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

```
show whitelist all
```

Syntax Description

<code>show</code>	Display information
<code>whitelist</code>	Display whitelist information
<code>all</code>	All whitelists

Defaults

None.

Example

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

ruckus#
```

show whitelist name

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

```
show whitelist name <WORD>
```

Syntax Description

show	Display information
whitelist	Display whitelist information
name <WORD>	Specify the name of the whitelist

Defaults

None.

Example

```
ruckus# show whitelist name "printer whitelist"
```

```
White Lists:
```

```
  ID:
```

```
    1:
```

```
      Name= printer whitelist
```

```
      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 Master.

show l3acl all

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

```
show l3acl all
```

Syntax Description

show	Display information
------	---------------------

l3acl1 Display L3 ACL information

all All L3 ACL

Defaults

None.

Example

```
ruckus# show l3acl all
L3/L4/IP ACL:
ID:
4:
Name= test2
Description= test2
Default Action if no rule is matched= Deny all by default
Rules:
Order= 1
Description=
Type= Allow
Destination Address= Any
Destination Port= 53
Protocol= Any
Order= 2
Description=
Type= Allow
Destination Address= Any
Destination Port= 67
Protocol= Any
Order= 3
Description=
Type= Allow
Destination Address= 8.8.8.8/24
Destination Port= 25
Protocol= 6
```

show l3acl name

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

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

Syntax Description

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

Defaults

None.

Example

```
ruckus# show l3acl name test2
L3/L4/IP ACL:
ID:
4:
Name= test2
Description= test2
Default Action if no rule is matched= Allow all by default
Rules:
Order= 1
Description=
Type= Allow
Destination Address= Any
Destination Port= 53
Protocol= Any
Order= 2
Description=
Type= Allow
Destination Address= Any
Destination Port= 67
Protocol= Any
Order= 3
Description=
Type= Allow
Destination Address= 8.8.8.8/24
Destination Port= 25
Protocol= 6
```

Show Hotspot Commands

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

show hotspot all

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

```
show hotspot all
```

Syntax Description

<code>show</code>	Display information
<code>hotspot</code>	Display hotspot information
<code>all</code>	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
      White List = No ACLS
      Location ID=
```

```
Location Name=  
Walled Garden 1= 1.1.1.1  
IPv4 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
White List = No ACLS
Location ID=
Location Name=
Walled Garden 1= 1.1.1.1
IPv4 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 authentication
    Multiple users to share a single guest pass = Disallowed
  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
```

```
ruckus#
```

Show Role Commands

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

show role all

To display a list of all roles that have been created on the Master, 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= Allowed
```

```
        Allow Unleashed Administration= Super Admin
```

```
      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= Allowed
        Allow Unleashed Administration= Super Admin
      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 Master.

show user all

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

```
show user all
```

Syntax Description

<code>show</code>	Display information
<code>user</code>	Display user information
<code>all</code>	All existing user accounts

Defaults

None.

Example

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

show user name

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

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

Syntax Description

<code>show</code>	Display information
<code>user name</code>	Display user information
<code><WORD></code>	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 Master 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

<code>show</code>	Display information
<code>current-active-clients</code>	Display currently active wireless clients
<code>all</code>	All active wireless clients

Defaults

None.

Example

```
ruckus# show current-active-clients all
Mac Address= 84:2e:27:e7:df:53
OS/Type= Android
Host Name= android-66f67a0b340e272d
```



```
User/IP= 172.18.151.10
Role=
Access Point= 6c:aa:b3:3d:66:30
BSSID= 6c:aa:b3:7d:66:38
Connect Since=2017/02/20 07:28:44
Auth Method= OPEN
WLAN= ggk_wlan_ok
VLAN= 1
Channel= 1
Radio= 802.11gn
Signal= 62
Status= Authorized

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	Display currently active wireless clients
mac <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= 3c:a9:f4:77:4a:f0
OS/Type= Windows 7/Vista
Host Name= sdc-ggk-PC
User/IP= 172.18.151.5
```

```
Role=  
Access Point= 6c:aa:b3:3d:66:30  
BSSID= 6c:aa:b3:7d:66:3c  
Connect Since=2017/02/20 06:10:10  
Auth Method= OPEN  
WLAN= ggk_wlan_ok  
VLAN= 1  
Channel= 157  
Radio= 802.11an  
Signal= 60  
Status= Authorized  
Received from client= 1473 pkts / 172943 bytes  
Transmitted to client= 18590 pkts / 1946685 bytes  
Tx. drops due to retry failure= 0 pkts  
  
...  
ruckus#
```

Show Mesh Commands

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

show mesh info

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

```
show mesh info
```

Syntax Description

<code>show</code>	Display information
<code>mesh</code>	Display mesh network information
<code>info</code>	Show mesh information

Defaults

None.

Example

```
ruckus# show mesh info
Mesh Settings:
Mesh Status= Enabled
Mesh Name (ESSID)= Mesh-000000000311
Mesh Passphrase= GdxW5CUgrn_SEHOPyCSxv_cQHScA MH-OpnRGfX sRvwXBjL-
wUsD6eeK8CMEZfm
Mesh Hop Detection:
Status= Disabled
Mesh Downlinks Detection:
Status= Disabled
Tx. Rate of Management Frame=2Mbps
Beacon Interval= 200ms
ruckus#
```

show mesh topology

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

```
show mesh topology
```

Syntax Description

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

Defaults

None.

Example

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

```
ruckus#
```

Show Dynamic PSK Commands

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

```
show dynamic-psks
```

Syntax Description

<code>show</code>	Display information
<code>dynamic-psks</code>	Display dynamic PSKs that have been generated

Defaults

None.

Example

```
ruckus# show dynamic-psks  
Generated Dynamic PSKs:  
DPSK:  
User= BatchDPSK_User_1  
Mac Address= 00:00:00:00:00:00  
Created= 2011/03/01 03:30:01  
Expired= Unlimited  
DPSK:  
User= BatchDPSK_User_2  
Mac Address= 00:00:00:00:00:00  
Created= 2011/03/01 03:30:02  
Expired= Unlimited  
DPSK:  
User= DPSK-User-2  
Mac Address= 00:11:22:33:44:55  
Created= 2011/03/01 03:30:47  
Expired= Unlimited
```

Show Dynamic Certificate Commands

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

```
show dynamic-certs
```

Syntax Description

<code>show</code>	Display information
<code>dynamic-certs</code>	Display dynamic certificates that have been generated

Defaults

None.

Example

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

Show Guest Pass Commands

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

```
show guest-passes
```

Syntax Description

<code>show</code>	Display information
<code>guest-passes</code>	Display guest passes that have been generated

Defaults

None.

Example

```
ruckus# show guest-passes  
Generated Guest Passes:  
ID:  
Guest Name= John Doe  
Remarks=  
  
Expires= 2017/01/11 08:32:15  
Re-auth=
```

```

Creator= ruckus
Sharable= No
Wlan= Ruckus-Guest

```

```
ruckus#
```

Show Events and Activities Commands

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

```
show events-activities
```

Syntax Description

<code>show</code>	Display information
<code>events-activities</code>	Display a list of events and activities records by the Master

Defaults

None.

Example

```

ruckus# show events-activities
ruckus# show events-activities
Last 300 Events/Activities:
Activitiy:
Date/Time= 2017/08/09 08:51:14
Severity= High
User=
Activities= AP[ruckus-ap] Radio [5G] Enabled, time
[Wed Aug 9 08:51:14 2017]
Activitiy:
Date/Time= 2017/08/09 08:51:14
Severity= High
User=
Activities= AP[ruckus-ap] Radio [2.4G] Enabled, time [Wed Aug
9 08:51:13 2017]
Activitiy:
Date/Time= 2017/08/09 08:50:10

```

Severity= Low

Show Alarm Commands

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

```
show alarm
```

Syntax Description

<code>show</code>	Display information
<code>alarm</code>	Display a list of alarms that have been generated by the Master

Defaults

None.

Example

```
ruckus# show alarm
Last 300 Alarms:
  Alarms:
    Date/Time= 2017/08/09 08:51:14
    Name= AP Radio On
    Severity= High
    Activities= AP[ruckus-ap] Radio [5G] Enabled, time [Wed Aug
9 08:51:14 2017]
...
ruckus#
```

Show License Commands

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


```
show license
```

Syntax Description

show	Display information
license	Display the Master's license information

Defaults

None.

Example

```
ruckus# show license
License:
  Model= R500
  Max. AP Number= 25
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 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.)

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
```

Configuring Master Settings

3

In this chapter:

- Configuration Commands Overview
- General Config Commands
- Configure Context Show Commands
- Configure AAA Server Commands
- Configure DHCP Server Commands
- Configure Admin Commands
- Configure Access Points Commands
- Configure AP Policy Commands
- Configure AP Group Commands
- Configure System Commands
- Configure WLAN Settings Commands
- Configure User Commands
- Configure Hotspot Commands
- Configure Mesh Commands
- Configure Alarm Commands
- Configure Services Commands
- Configure WIPS Commands
- Configure mDNS (Bonjour) Commands

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 settings.

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 whitelist

Displays a list of client isolation white lists.

show dvcpcy

Displays a list of Device Policies.

show load-balancing

Displays information about Load balancing.

show wlan

Displays a list of all WLAN services (Names).

show wlan-group

Displays a list of existing WLAN groups.

show role

Displays a list of roles.

show user

Displays a list of users.

show hotspot

Displays a list of hotspot entries.

show guest-access-service

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

```
show guest-access-service [all|name<WORD>]
```

show ap-group

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

```
show ap-group [all|name<WORD>]
```

show ap-policy

Displays the ap policy 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>
```


Configure AAA Server Commands

This section describes the commands that you can use to configure AAA server entries on the Master. 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

<code>abort</code>	Exits the config-aaa context without saving changes.
<code>end</code>	Saves changes, and then exits the config-aaa context.
<code>exit</code>	Saves changes, and then exits the config-aaa context.
<code>quit</code>	Exits the config-aaa context without saving changes.
<code>name <WORD></code>	Sets the AAA server name.
<code>show</code>	Displays a list of available AAA servers.
<code>type</code>	Sets the type of AAA server.
<code>type ad</code>	Sets the AAA server type to 'Active Directory'.
<code>type radius-auth</code>	Sets the AAA server type to 'RADIUS'.
<code>type radius-acct</code>	Sets the AAA server type to 'RADIUS Accounting'.
<code>radius-encryption tls</code>	Sets the AAA server encryption type to TLS'.
<code>auth-method pap</code>	Sets the authentication method to PAP.
<code>auth-method chap</code>	Sets the authentication method to CHAP.
<code>ip-addr <IP-ADDR></code>	Sets the AAA server's IP/IPv6 address.
<code>port <PORT-NUM></code>	Sets the AAA server's port.

no radius-encryption	Disables the AAA server encryption.
no ad-global-catalog	Disables global catalog support.
no encryption-TLS	Disable the TLS Encryption
no backup	Disables the backup function.
ad-global-catalog	Enables global catalog support.
admin-dn <WORD>	Sets the admin domain name.
admin-password <WORD>	Set the admin password.
radius-secret <WORD>	Sets the AAA 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>	
retry-count <NUMBER>	Sets the failover request timeout(2-20 seconds)
consecutive-drop- packet <NUMBER>	Sets the failover retry count (2~10 times).
reconnect-primary- interval <NUMBER>	Sets the number of consecutive dropped packet (range:1~10 , default is 1). Sets the failover re-connect to primary interval (1~86400 minutes).

Example

```
ruckus(config)# aaa radius_aaa
```

The AAA server 'radius_aaa' has been created. To save the AAA server, type 'end' or 'exit'.

```
ruckus(config-aaa)# type radius-auth
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

```
ruckus(config-aaa)# ip-addr 172.18.151.3
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

```
ruckus(config-aaa)# port 1812
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

```
ruckus(config-aaa)# radius-secret bbbbbb
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

```
ruckus(config-aaa)# auth-method chap
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

```
ruckus(config-aaa)# show
```

```
AAA:
  ID:
    :
    Name= radius_aaa
    Type= RADIUS server
    Auth Method= chap
    Primary RADIUS:
      IP Address= 172.18.151.3
      Port= 1812
      Secret= *****
    Secondary RADIUS:
      Status= Disabled
    Retry Policy:
      Request Timeout= 3 Seconds
  Max. Number of Retries= 2 Times
```

```
ruckus(config-aaa)# end
```

The AAA server ' radius_aaa' 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 Master. 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

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

Defaults

none

Example

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

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

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

ruckus(config)#
```

no dhcp

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

```
no dhcp <WORD>
```

Example

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

show

Displays a list of available DHCP servers.

```
show
```

name

Sets the DHCP server name.

```
name <WORD>
```

description

Sets the DHCP server description.

```
description <WORD>
```

first

Sets the DHCP server's first IP address.

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

second

Sets the DHCP server's second IP address.

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

no second

Deletes the DHCP server's second IP address.

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

Configure Admin Commands

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

admin

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

```
admin
```

Example

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

name

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

```
name <WORD>
```

Syntax Description

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

Defaults

admin

Example

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

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

The command was executed successfully. To save the changes, type 'end' or 'exit'.

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

The administrator preferences have been updated.

Your changes have been saved.

```
ruckus(config)#
```

name password

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

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

Syntax Description

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

Defaults

admin

Example

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

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

The command was executed successfully. To save the changes, type 'end' or 'exit'.

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

The administrator preferences have been updated.

Your changes have been saved.
ruckus(config)#

Admin Authentication Commands

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

auth-server

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

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

Syntax Description

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

Defaults

None.

Example

```
ruckus(config-admin)# auth-server radius
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

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

no auth-server

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

```
no auth-server
```

Syntax Description

<code>no auth-server</code>	Disable admin authentication with an external server
-----------------------------	--

Defaults

None.

Example

```
ruckus(config-admin) # no auth-server
```

The command was executed successfully.

auth-server with-fallback

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

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

Syntax Description

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

Defaults

None.

Example

```
ruckus(config-admin) # auth-server radius with-fallback
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

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

```
Administrator Name/Password:
```

```
Name= admin
```

```
Password= admin
```

```
Authenticate:
```

```
Mode= Authenticate with authentication server 'radius'
```

```
Fallback= Enabled
```

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

Configure Access Points 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 6c:aa:b3:3d:66:30  
The AP '6c:aa:b3:3d:66:30' has been loaded. To save the AP, type  
'end' or 'exit'.  
ruckus(config-ap)# devname R500-Unleashed  
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
```

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")

Defaults

none

Example

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

Radio 2.4/5 GHz Commands

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

radio

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

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

Syntax Description

2.4	Configure the 2.4 GHz radio
5	Configure the 5 GHz radio
channelization [auto]<NUMBER>]	admission-control <VALUE>
channel [auto]<NUMBER>]	spectralink- compatibility [enable disable]
tx-power [auto full min num <1- 10>]	

Set channel width	channel
to 20 MHz, 40	Set transmit power to auto, full, min, or a number (-1 dB~-10dB)
MHz or Auto Set	Set the radio to use the specified call admission control airtime usage limit (%)
channel to Auto or	Enable SpectraLink Compatibility on the specified radio (set DTIM=2, minrate=5.5Mbps and enable RTS-CTS protection mode)
manually set	

channel-range <NUMBER-LIST>	Set the allowed list of channels for the specified radio
<hr/>	
wlan-group <WORD>	Set the AP radio as a member of a WLAN group
<hr/>	
wlan-service [enable disable]	Enable WLAN service on this radio
<hr/>	
wlan-service-override	Enable the override of the WLAN service settings for this radio
<hr/>	
extant-gain <NUMBER>	Set external antenna gain (on APs that support external antennas) (dBi)

Defaults

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

Example

```
ruckus(config-ap) # radio 2.4 channelization auto
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

```
ruckus(config-ap) # radio 2.4 channel auto
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

```
ruckus(config-ap) # radio 2.4 wlan-group Default
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

```
ruckus(config-ap) # radio 2.4 wlan-service
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

```
ruckus(config-ap) # radio 2.4 tx-power auto
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

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

The device information has been updated.

Your changes have been saved.

```
ruckus(config)#
```

no radio

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

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

Syntax Description

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

Example

```
ruckus(config-ap) # no radio 2.4 tx-power-override
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

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

mesh mode

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

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

Syntax Description

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

Defaults

Auto.

Example

```
ruckus(config-ap) # mesh mode auto
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

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

mesh uplink-selection

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

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

Syntax Description

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

Defaults

Auto.

Example

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

The command was executed successfully. To save the changes, type 'end' or 'exit'.

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

Example

```
ruckus(config-ap) # mesh uplink-selection auto
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

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

status-leds

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

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

Defaults

Enabled.

Syntax Description

<code>status-leds</code>	Configure status LEDs
<code>enable</code>	Override group config, enable status LEDs
<code>disable</code>	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
```

usb-port

To disable the override the group configuration and enable/disable the USB port for this AP, use the following command:

```
usb-port [enable|disable]
```

no usb-port-override

To disable the override of the USB port for the specified AP model, use the following command:

```
no usb-port-override
```

poe-out

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

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

Defaults

Disabled.

Syntax Description

<code>poe-out</code>	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] [gain
<NUMBER>] cable-loss <NUMBER> [2-antennas|3-antennas]
```

Syntax Description

2.4G	Configure external 2.4GHz antenna
5G	Configure external 5GHz antenna
enable disable	Enable/disable external antenna
gain	Set external antenna gain for 2.4/5GHz radio
cable-loss <NUMBER>	Enter the external antenna loss (0-90 dB)
2-antennas	Select two external antennas for the specified radio
3-antennas	Select three external antennas for the specified radio

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

<code>internal-heater</code>	Configure internal heater
<code>enable</code>	Override group config, enable internal heater
<code>disable</code>	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

<code>cband-channels</code>	Configure C-band channels
<code>enable</code>	Override group config, enable C-band channels
<code>disable</code>	Override group config, disable C-band channels

Example

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

no cband-channels-override

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

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

usb-software

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

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

no usb-software

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

```
no usb-software
```

radio-band

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

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

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

Syntax Description

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

Example

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

no radio-band-override

To disable 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.

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) #
```

show

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

```
show
```

Example

```
ruckus(config)# ap 6c:aa:b3:3d:66:30
```

The AP '6c:aa:b3:3d:66:30' has been loaded. To save the AP, type 'end' or 'exit'. ruckus(config-ap)# **show**

```
AP:
```

```
ID: 1
```

```
MAC Address= 6c:aa:b3:3d:66:30
```

```
Model= r500
Approved= Yes
Device Name= R500-Unleashed
Device Role= Member
Description= ggk_unleashed
Location= un
GPS=
CERT = Normal
Bonjour-policy=
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
        SpectraLink Compatibility=
Disabled
    Radio b/g/n:
        Channelization= Auto
```

```
Channel= Auto
WLAN Services enabled= Yes
Tx. Power= Auto
WLAN Group Name= Default
Call Admission Control=
OFF
SpectraLink Compatibility=
Disabled
Override global ap-model port
configuration= No
Network Setting:
    Protocol mode= IPv4-Only
    Device IP Settings= Manual
    IP Address= 172.18.151.1
    Netmask= 255.255.255.0
    Gateway=
    Primary DNS Server=
172.18.100.35
    Secondary DNS Server=
172.18.100.45
Mesh:
    Status= Enabled
    Mode= Auto
    max hops= unlimited
Uplink:
    Status= Smart
LLDP:
    Status = Enabled
    Interval = 30
```

```
HoldTime = 120
Mgmt = Enabled
Ports:
    Send out LLDP packet on
eth0 = Enabled
    Send out LLDP packet
on eth1 = Enabled
Venue Name List:
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

ruckus(config-ap)#
```


Configure AP Group Commands

This section describes the commands that you can configure the default AP groups on the Master. 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 configure an default AP group and enter the `config-apgrp` context, for Unleashed product, only “System Default” is supported, enter the following command:

```
ap-group <System Default>
```

Syntax Description

<code>ap-group</code>	Configure an AP group
<code><WORD></code>	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)#
```

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
```

Defaults

None

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)# show
```

```
APGROUP:
```

```
ID:
```

```
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(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
```

Radio 2.4/5 GHz Commands

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

radio

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

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

Syntax Description

radio	Configure AP group radio settings
2.4	Configure 2.4 GHz radio
5	Configure 5 GHz radio
no	Disables settings for the specified radios in the AP group
channel	Set radio channel (Auto or number) channelization
	Set radio channel width (Auto, 20MHz or 40MHz)
auto-channel-selection [four-channel three- channel]	Set auto channel selection to four-channel (1,5,9,13) or three-channel (1,6,11)
tx-power	Set radio transmit power (Auto, Full, 1/2, 1/4, 1/8, Min) or <NUMBER> (-1dB~-10dB)
11n-only	Set radio 11n-only mode to Auto or N-only
spectralink- compatibility	Enable SpectraLink Compatibility settings on the radio (sets DTIM=2, minrate=5.5Mbps and enable RTS-CTS protection mode)

wlan-service Disable or enable WLAN service on the radio

Defaults

Channel: Auto
Channelization: Auto
Auto-Channel Selection: Three-channel
TX Power: Auto
11n-only: Auto
WLAN group: Default
Admission Control: Off
SpecraLink Compatibility: Off
WLAN Service: Enabled

Example

```
ruckus(config)# ap-group "System Default"
The AP group entry 'System Default' has been loaded. To save the
AP group, type 'end' or 'exit'.
ruckus(config-apgrp)# radio 2.4 channel auto
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-apgrp)# radio 5 channelization auto
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-apgrp)# radio 5 11n-only N-only
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-apgrp)# radio 5 wlan-group Default
The command was executed successfully. To save the changes, type
'end' or 'exit'.
ruckus(config-apgrp)# radio 2.4 tx-power Num 1
The command was executed successfully. To save the changes, type
'end' or 'exit'.

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

radio 2.4 channel auto

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

radio 2.4 channel number <NUMBER>

Sets the 2.4GHz radio to use the specified channel.

radio 2.4 channelization auto

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

radio 2.4 channelization number <NUMBER>

Sets the 2.4GHz radio to use the specified channelization.

radio 2.4 auto-channel-selection four-channel

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

radio 2.4 auto-channel-selection three-channel

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

radio 2.4 tx-power Auto

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

radio 2.4 tx-power Full

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

radio 2.4 tx-power 1/2

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

radio 2.4 tx-power 1/4

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

radio 2.4 tx-power 1/8

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

radio 2.4 tx-power Min

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

radio 2.4 tx-power Num

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

radio 2.4 11n-only Auto

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

radio 2.4 11n-only N-only

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

radio 2.4 wlan-group <WORD>

Assigns the 2.4GHz radio to the specified WLAN group.

radio 2.4 admission-control <VALUE>

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

radio 2.4 spectralink-compatibility [enable | disable]

Enables the SpectraLink Compatibility on 2.4GHz radio (will set DTIM=2, minrate=5.5Mbps and enable RTS-CTS protection mode).

radio 2.4 wlan-service [enable | disable]

Enables or disables the WLAN service on the 2.4GHz radio.

radio 2.4 channel-range <NUMBER-LIST>

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

radio 5 indoor channel auto

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

radio 5 indoor channel number <NUMBER>

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

radio 5 indoor channel-range <NUMBER-LIST>

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

radio 5 outdoor channel auto

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

radio 5 outdoor channel number <NUMBER>

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

radio 5 outdoor channel-range <NUMBER-LIST>

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

radio 5 channel auto

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

radio 5 channel number <NUMBER>

Sets the 5GHz radio to use the specified channel.

radio 5 channelization auto

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

radio 5 channelization number <NUMBER>

Sets the 5GHz radio to use the specified channelization.

radio 5 tx-power Auto

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

radio 5 tx-power Full

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

radio 5 tx-power 1/2

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

radio 5 tx-power 1/4

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

radio 5 tx-power 1/8

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

radio 5 tx-power Min

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

radio 5 tx-power Num

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

radio 5 11n-only Auto

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

radio 5 11n-only N-only

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

radio 5 wlan-group <WORD>

Assigns the 5GHz radio to the specified WLAN group.

radio 5 admission-control <VALUE>

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

radio 5 spectralink-compatibility [enable | disable]

Enables the SpectraLink Compatibility on 5GHz radio (will set DTIM=2, minrate=5.5Mbps and enable RTS-CTS protection mode).

radio 5 wlan-service [enable | disable]

Enables or disables the WLAN service on the 5GHz radio.

no radio 2.4 channelization-override

Disables the override of the 2.4GHz channelization settings.

no radio 2.4 channel-range-override

Disables the override of the 2.4GHz channel range settings.

no radio 2.4 channel-override

Disables the override of the 2.4GHz channel settings.

no radio 2.4 tx-power-override

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

no radio 2.4 11n-only-override

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

no radio 2.4 wlan-group-override

Disables the override of the 2.4GHz WLAN group settings.

no radio 2.4 admission-control

Disables call admission control function on the 2.4GHz radio.

no radio 2.4 admission-control-override

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

no radio 2.4 spectralink-compatibility-override

Disables the override of the 2.4GHz SpectraLink Compatibility settings.

no radio 2.4 wlan-service-override

Disables the override of the 2.4GHz WLAN service settings.

no radio 5 indoor channel-range-override

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

no radio 5 indoor channel-override

Disables the override of the 5GHz indoor channel settings.

no radio 5 outdoor channel-range-override

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

no radio 5 outdoor channel-override

Disables the override of the 5GHz outdoor channel settings.

no radio 5 channelization-override

Disables the override of the 5GHz channelization settings.

no radio 5 tx-power-override

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

no radio 5 11n-only-override

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

no radio 5 wlan-group-override

Disables the override of the 5GHz WLAN group settings.

no radio 5 admission-control

Disables call admission control function on the 5GHz radio.

no radio 5 admission-control-override

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

no radio 5 spectralink-compatibility-override

Disables the override of the 5GHz SpectraLink Compatibility settings.

no radio 5 wlan-service-override

Disables the override of the 5GHz WLAN service settings.

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 (e.g., R500, R510, R610, R710, T300, etc.)
status-leds	Configures the status LEDs for the specified AP model (enable, disable).
max-clients <NUMBER>	Sets the maximum clients for the AP

Defaults

Status LEDs: Enabled

PoE Out: Disabled

Internal Heater: Disabled

C-band channels: Disabled

USB Ports: Enabled

Power Mode: Default

Example

```
ruckus(config-apgrp)# model r500 status-leds enable  
ruckus(config-apgrp)# end  
The AP group 'System Default' has been updated.  
Your changes have been saved.  
ruckus(config)#
```

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
```

Syntax Description

abort	Exit the <code>config-l2acl</code> context without saving changes
-------	---

Defaults

None.

Example

```
ruckus(config-l2acl)# abort  
No changes have been saved.  
ruckus(config)#
```

end

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

```
end
```

Syntax Description

end	Save changes and exit the <code>config-l2acl</code> context
-----	---

Defaults

None.

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
```

Syntax Description

exit	Save changes and exit the <code>config-l2acl</code> context
------	---

Defaults

None.

Example

```
ruckus(config-l2acl)# exit  
The L2 ACL entry has saved successfully.  
Your changes have been saved.  
ruckus(config)#
```

quit

To exit the `config-12acl` context without saving changes, use the following command:

```
quit
```

Syntax Description

quit	Exit the <code>config-12acl</code> context without saving changes
------	---

Defaults

None.

Example

```
ruckus(config-12acl)# 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-12acl` context.

```
show
```

Syntax Description

show	Display the Layer 2 access control list settings
------	--

Defaults

None.

Example

```
ruckus(config-12acl)# show  
L2/MAC ACL:  
ID:  
:  
Name= 12acl1  
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>
```

Syntax Description

add mac	Add a MAC address to the ACL
<MAC>	Add 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.

ConfigureLayer3AccessControlCommands

Use the `l3acl` commands to configure the Layer 3 Access Control List settings. To run these commands, you must first enter the `config-l3acl` or `config-l3acl-ipv6` context.

l3acl

To enter the `config-l3acl` context, run this command:

```
l3acl <WORD>
```

Syntax Description

<code>l3acl</code>	Create or configure a Layer 3 Access Control List
<code><WORD></code>	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
```

Syntax Description

abort	Exit the context without saving changes
-------	---

Defaults

None.

Example

```
ruckus(config-l3acl)# abort  
No changes have been saved.  
ruckus(config)#
```

end

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

```
end
```

Syntax Description

end	Save changes and exit the context
-----	-----------------------------------

Defaults

None.

Example

```
ruckus(config-l3acl)# end  
The L3/L4/IP ACL entry has saved successfully.  
Your changes have been saved.  
ruckus(config)#
```

exit

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

```
exit
```

Syntax Description

exit	Save changes and exit the context
------	-----------------------------------

Defaults

None.

Example

```
ruckus# config-l3acl  
ruckus(config-l3acl)# exit  
Your changes have been saved.
```

quit

To exit the `config-l3acl` context without saving changes, use the following command:

```
quit
```

Syntax Description

quit Exit the context without saving changes

Defaults

None.

Example

```
ruckus(config-l3acl)# quit
No changes have been saved.
ruckus(config)#
```

show

To display the L3ACL settings, use the `show` command. You must run this command from within the `config-l3acl` context.

```
show
```

Syntax Description

show	Display the Layer 3 access control list settings
------	--

Defaults

None.

Example

```
ruckus(config-l3acl)# show
L3/L4/IP ACL:
ID:
3:
Name= test_newname
Description= justfortestCLI
Default Action if no rule is matched= Deny all by default
Rules:
Order= 1
Description=
Type= Allow
Destination Address= Any
Destination Port= 53
Protocol= Any
Order= 2
```

```
Description=  
Type= Allow  
Destination Address= Any  
Destination Port= 67  
Protocol= Any
```

name

To set the name of an L3/L4/IP ACL entry, use the following command:

```
name <WORD>
```

Syntax Description

name	Set the name of an L3/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'.

no rule-order

To delete a rule from the L3/L4/IP ACL, use the following command:

```
no rule-order <NUMBER>
```

Syntax Description

no rule-order	Delete a rule from the L3/L4/IP ACL
<NUMBER>	Delete this rule ID

Defaults

None.

Example

```
ruckus(config-l3acl)# no rule-order 3  
The rule '3' has been removed from the ACL.
```

rule-order

To create or modify a rule in the L3/L4/IP ACL, use the following command:

```
rule-order <NUMBER>
```

Syntax Description

rule-order	Create a new rule or modify an existing one
<NUMBER>	Create or modify this rule ID

Defaults

None.

Example

For example, to set the current rule as the third ACL rule to apply, use the following command:

```
ruckus(config-l3acl)# rule-order 3  
ruckus(config-l3acl-rule)#
```

Layer 3 Access Control Rule Commands

Use the `l3acl-rule` commands to configure the Layer 3/Layer 4/IP Access Control List rules. To run these commands, you must first enter the `config-l3acl-rule` context. To enter the `config-l3acl-rule` context, run this command:

```
rule-order <NUMBER>
```

end

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

```
end
```

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 Whitelist Commands

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

whitelist

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

```
whitelist <WORD>
```

no whitelist

To delete a whitelist entry, use the following command:

```
no whitelist <WORD>
```

name

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

```
name <WORD>
```

description

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

```
description <WORD>
```

Configuring Whitelist Rules

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

rule

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

```
rule <NUMBER>
```

no rule

To delete a whitelist rule, use the following command:

```
no rule <NUMBER>
```

description

To set the White 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 Master'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

Enable the band balancing settings.

disable

Disables the band balancing settings.

percent-2.4G <NUMBER>

Configures percent of clients on 2.4G band.

show

Displays information about Band balancing.

Example

```
ruckus(config)# band-balancing
ruckus(config-band-balancing)# enable
The band balancing settings have been updated.
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
Band Balancing:
  Status= Enabled
  Percent of clients on 2.4G band: 25%

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


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 Master'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)#
```

no load-balancing

To disable load balancing settings (from the `config` context), use the following command:

```
no load-balancing
```

Example

```
ruckus(config)# no load-balancing  
The load balancing settings have been updated.  
ruckus(config)# show load-balancing
```

Load Balancing:

Status= Disabled

Radio:

0:

AdjacentThreshold= 50

WeakBypass= 33

StrongBypass= 55

ActivationThreshold= 10

NewTrigger= 3

Headroom= 3

1:

AdjacentThreshold= 43

```
WeakBypass= 35  
StrongBypass= 55  
ActivationThreshold= 10  
NewTrigger= 3  
Headroom= 3
```

```
ruckus(config)#
```

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

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

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

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:
```

```
  Status= Disabled
```

```
Radio:
```

```
  0:
```

```
    AdjacentThreshold= 50
```

```
    WeakBypass= 33
```

```
    StrongBypass= 55
```

```
    ActivationThreshold= 1
```

```
    NewTrigger= 3
```

```
    Headroom= 3
```

```
  1:
```

```
AdjacentThreshold= 43  
WeakBypass= 35  
StrongBypass= 55  
ActivationThreshold= 10  
NewTrigger= 3  
Headroom= 3
```

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

Configure System Commands

Use the `sys` or `system` command to configure the Master'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 Master's country code, use the following command:

```
dot11-country-code <COUNTRY-CODE> {arguments}
```

Syntax Description

<code>dot11-country-code</code>	Configure the Master'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 Unleashed Outdoor APs to use channels regulated as indoor use-only
not-allow-indoor	Disallows Unleashed 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# config
ruckus(config)# system
ruckus(config-sys)# dot11-country-code US
The country code settings have been updated.
ruckus(config-sys)#
```

hostname

To set the system hostname, use the following command:

```
hostname
```

Syntax Description

hostname	Set the Master'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 Master'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 name-server

To set the Master'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

<code>ip name-server</code>	Configure the Master's DNS server address or addresses
<code>DNS-ADDR</code>	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 Master'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 Master's IP address and netmask
<IP-ADDR>	Set the Master's IP address to this value
<NET-MASK>	Set the Master'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 Master's IP address mode, use the following command:

```
ip mode <dhcp|static>
```

Syntax Description

ip mode	Configure the Master's IP address mode
dhcp	Set the Master's IP address mode to DHCP
static	Set the Master's IP address mode to static

Defaults

None.

Example

To set the Master'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
```

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

no ip

To disable IPv4 addressing, use the following command:

```
no ip
```

no ntp

To disable the NTP client, use the following command:

```
no ntp
```

Syntax Description

no ntp	Disable the NTP client on the Master.
--------	---------------------------------------

Defaults

Enabled. The default NTP server addresss is `ntp.ruckuswireless.com`.

Example

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

ntp

To enable the NTP client, use the following command:

```
ntp <IP-ADDR/DOMAIN-NAME>
```

Syntax Description

ntp	Enable the NTP client
-----	-----------------------

<IP-ADDR/ DOMAIN-NAME>	Set the NTP server address to this IP address/domain name
---------------------------	--

Defaults

None.

Example

```
ruckus(config-sys)# ntp 192.168.2.21
```

The NTP settings have been updated.

```
ruckus(config-sys)# ntp sohu.com
```

The NTP settings have been updated.

timezone

To configure time zone settings, use the following command:

```
timezone <TIMEZONE>
```

Defaults

GMT+0

Example

```
ruckus(config-sys)# timezone +8
```

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 anonymous access, use the following command:

```
no ftp-anon
```

ftp

Enable FTP server.

no ftp

Disable FTP server.

Management Interface Commands

To configure management interface settings, you must first enter the `config-sys-mgmt-if` context from the `config-sys` context.

mgmt-if

To enter the `config-sys-mgmt-if` context and configure the management interface settings, use the following command:

```
mgmt-if
```

Syntax Description

<code>mgmt-if</code>	Configure the management interface settings
----------------------	---

Defaults

None.

Example

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

no mgmt-if

To disable the management interface, use the following command:

```
no mgmt-if
```

Syntax Description

<code>no mgmt-if</code>	Disable the management interface
-------------------------	----------------------------------

Defaults

None.

Example

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

ip addr

To set the management interface IP address, use the following command:

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

flexmaster

To set the FlexMaster server address and the periodic inform interval, use the following command:

```
flexmaster <IP-ADDR/DOMAIN-NAME> interval <NUMBER>
```

Syntax Description

flexmaster	Configure the FlexMaster server settings
<IP-ADDR/DOMAIN-NAME>	Set to this URL or IP address
interval	Configure the periodic inform interval
<NUMBER>	Set to this interval (in minutes)

Defaults

None.

Example

```
ruckus(config-sys)# flexmaster http://172.18.30.118 interval 30  
The FlexMaster Management settings have been updated.
```

no flexmaster

To disable FlexMaster management of the controller, use the following command:

```
no flexmaster
```

Syntax Description

no flexmaster	Disable FlexMaster management of the controller
---------------	---

Defaults

None

Example

```
ruckus(config-sys)# no flexmaster
FlexMaster Management has been disabled.
```

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.
contact <WORD>	Enables SNMPV2 agent and sets the system contact. location <WORD> sets the system location
ro-community	<WORD>

rw-community	Enables SNMPV2 agent and sets the RO community name.
<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

<code>rw-community</code>	Configure the read-write community name
<code><WORD></code>	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
```

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	
ro-user <WORD> SHA <WORD>	Sets the privacy to None for SNMPV3.
ro-user <WORD> SHA <WORD> DES <WORD>	Contains commands that can be executed from within the context.
ro-user <WORD> SHA <WORD> AES <WORD>	Sets the privacy phrase of DES for SNMPV3.
ro-user <WORD> SHA <WORD> None	Sets the privacy phrase of AES for SNMPV3.
	Sets the privacy to None for SNMPV3.
rw-user <WORD>	Contains commands that can be executed from within the context.
rw-user <WORD>	Contains commands that can be executed from within the context.
MD5 <WORD>	
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>	
rw-user <WORD> SHA <WORD> DES <WORD>	Contains commands that can be executed from within the context.
rw-user <WORD> SHA <WORD> AES <WORD>	Sets the privacy phrase of DES for SNMPV3.
rw-user <WORD> SHA <WORD> None	Sets the privacy phrase of AES for SNMPV3.
	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> <community>
```

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
<community>	Set the trap receiver community

Defaults

None

Example

```
ruckus(config-sys)# snmpv2-trap 1 192.168.10.22 public
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.

Syslog Settings Commands

Use the `syslog` commands to configure the Master's syslog notification settings. To run these commands, you must first enter the `config-sys` context.

no syslog

To disable syslog notification, use the following command:

```
no syslog
```

Syntax Description

<code>no syslog</code>	Disable syslog notification
------------------------	-----------------------------

Defaults

Disabled.

Example

```
ruckus# config  
ruckus(config)# system  
ruckus(config-sys)# no syslog
```

The command was executed successfully.

syslog

To enable syslog notifications and enter the `config-sys-syslog` context, use the

following command:

```
syslog
```

server

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

```
server <IP-ADDR>
```

Syntax Description

<code>server</code>	Set the syslog server IP address.
<code><IPADDR></code>	Send syslog notifications to this IP address.

Defaults

Disabled.

facility

To set the facility name, use the following command:

```
facility <FACILITY NAME>
```

Syntax Description

<code>facility</code> <code><FACILITY NAME></code>	Sets the syslog facility name (local0 - local7)
---	---

Defaults

Disabled.

priority

To set the syslog priority level, use the following command:

```
priority <PRIORITY LEVEL>
```

Syntax Description

<code>priority</code> <code><PRIORITY LEVEL></code>	Sets the syslog priority level(emerg, alert, crit, err, warning, notice, info, debug).
--	--

Defaults

Disabled.

ap-facility

To set the AP syslog facility name, use the following command:

```
ap-facility <FACILITY-NAME>
```

Syntax Description

`ap-facility <FACILITY-NAME>` Sets the AP syslog facility name (local0 - local7).

Defaults

Disabled.

ap-priority

To set the AP syslog priority level, use the following command:

```
ap-priority <PRIORITY LEVEL>
```

Syntax Description

`ap-priority` Sets the AP syslog priority level (emerg, alert, crit, err,

<PRIORITY LEVEL> 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)#
```

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)#
```

bypasscna

Use the following command to bypass Apple Captive Network Assistance (CNA) on iDevices and OS X machines.

```
bypasscna <WLAN-TYPE>
```

Syntax Description

bypasscna	Bypass Apple Captive Network Assistance (CNA) on iDevices and OS X machines
<WLAN-TYPE>	Enter the WLAN service type (web-auth, guestaccess, wispr)

Example

```
ruckus(config-sys)# bypasscna web-auth
```

no bypasscna

To disable the ignore Apple CNA feature, use the following command:

```
no bypasscna
```

Example

```
ruckus(config-sys)# no bypasscna
```

no syslog-ap

To disable external syslog server configuration for AP, use the following command:

```
no syslog-ap
```

Example

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

Management Access Control List Commands

Use the following commands to create or configure management ACLs and enter the `config-sys-mgmt-acl` or `config-sys-mgmt-acl-ipv6` contexts. These commands must be used from the `config-sys` context.

mgmt-acl

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

```
mgmt-acl <WORD>
```

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

Syntax Description

<code>mgmt-acl</code>	Create or configure a management ACL
<code><WORD></code>	Create or configure this management ACL

Defaults

None.

Example

```
ruckus(config-sys)# mgmt-acl mac11  
The management ACL 'mac11' 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).

show

To display management ACL settings, use the show command.

QoS Commands

Use the following commands to configure QoS settings on the Master. These commands must be executed from the config-sys context.

no qos

To disable QoS on the Master, use the following command:

```
no qos
```

Syntax Description

no qos	Disable QoS on the Master
--------	---------------------------

Defaults

None.

Example

```
ruckus(config-sys)# no qos  
Changes are saved!  
System QoS function has been disabled.
```

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)#
```

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)#
```

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 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.

no snmp-trap

To disable the SNMP trap notifications, use the following command:

```
no snmp-trap <NUMBER>
```

Syntax Description

<code>no snmp-trap</code>	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

<code>no snmpv2-trap</code>	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

<code>no snmpv3-trap</code>	Disables SNMP trap notification by index
-----------------------------	--

Example

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

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 WLAN Settings Commands

Use the `config-wlan` commands to configure the WLAN settings, including the WLAN's description, SSID, and its security settings. To run these commands, you must first enter the `config-wlan` context.

wlan

To create a WLAN or configure an existing WLAN, use the following command:

```
wlan <WORD/NAME>
```

Executing this command enters the `config-wlan` context.

Syntax Description

wlan	Configure a WLAN
<WORD/NAME>	Name of the WLAN service

Defaults

None.

Example

```
ruckus(config)# wlan ruckus2
The WLAN service 'ruckus2' has been created. To save the WLAN
service, type 'end' or 'exit'.
ruckus(config-wlan)#
```

abort

Exits the config-wlan context without saving changes.

end

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

exit

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

quit

Exits the config-wlan context without saving changes.

description

To set the WLAN service description, use the following command:

```
description <WORD>
```

Syntax Description

description	Configure the WLAN description
<WORD>	Set the WLAN description this value

Defaults

None.

Example

```
ruckus(config-wlan)# description unleashed_wlan
```

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> |  
social-media]
```

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
social-media	Set the WLAN type to social media.

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 social-media

To set the WLAN type to “Social Media”, use the following command:

```
type social-media
```

open none

To set the authentication method to 'open' and encryption method to 'none', use the following command:

```
open none
```

Syntax Description

open	Set the authentication method to 'open'
none	Set the encryption method to 'none'

Defaults

None.

Example

```
ruckus(config)# wlan 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 wpa2 passphrase algorithm AES

To set the authentication method to 'open', encryption method to 'WPA2', and algorithm to 'AES', use the following command:

```
open wpa2 passphrase <PASSPHRASE> algorithm AES
```

Syntax Description

open	Set the authentication method to 'open'
------	---

wpa2	Set the encryption method to WPA2
passphrase <PASSPHRASE>	Set the WPA2 passphrase to <PASSPHRASE>
algorithm AES	Set the encryption algorithm to AES

Defaults

None.

Example

```
ruckus(config)# wlan randy-wlansvc-01-open
```

The WLAN service 'randy-wlansvc-01-open' has been created. To save the WLAN service, type end or exit.

```
ruckus(config-wlan)# open wpa2 passphrase 12345678 algorithm AES
```

The command was executed successfully.

```
ruckus(config-wlan)#
```

mac none auth-server

To set the authentication method to 'MAC Address' and encryption method to 'none', use the following command:

```
mac none auth-server <WORD>
```

Syntax Description

mac	Set the authentication method to 'MAC Address'
none	Set the encryption method to 'none'
auth-server <WORD>	Set the authorization server address to <WORD>

Defaults

None.

Example

```
ruckus(config-wlan)# mac none auth-server Ruckus-Auth-01
```

The command was executed successfully.

```
ruckus(config-wlan)#
```

dot1x wpa2 algorithm AES auth-server

To set the authentication method to '802.1x EAP', encryption method to 'WPA2', and algorithm to 'AES', use the following command:

```
dot1x wpa2 algorithm AES auth-server [local | name <WORD>]
```

Syntax Description

dot1x	Set the authentication method to '802.1x'
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)#
```

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)#
```

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
```

social-media-login

To set the social media login, use the following command:

```
social-media-login <WORD>
```

social-media-login facebook-wifi

To set the social media login to Facebook WiFi, use the following command:

```
social-media-login facebook-wifi
```

social-media-login google

To set the social media login to Google/Google+, use the following command:

```
social-media-login google <WORD> <WORD>
```

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 <WORD> <WORD>
```

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)#
```

whitelist

To apply a client isolation whitelist to this WLAN, use the following command:

```
whitelist name <WORD>
```

no whitelist

To disable the whitelist for this WLAN, use the following command:

```
no whitelist
```

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
```

Example

```
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
```

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 Master 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)#
```

priority low

To set the WLAN priority to low, use the following command:

```
priority low
```

priority high

To set the WLAN priority to high, use the following command:

```
priority high
```

web-auth

To enable Web authentication, use the following command:

```
web-auth [local | name <WORD>]
```

Syntax Description

web-auth	Enable Web authentication
local	Use local database as auth server
name	Specify an external auth server
<WORD>	The AAA server to use for Web authentication

Defaults

None

Example

```
ruckus# config
ruckus(config)# wlan wlan-123
ruckus(config-wlan)# 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	Configure 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
----------------	-----------------------------------

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

Notes

Dynamic VLAN can be enabled or disabled in the following two conditions: 1) The authentication method is '802.1X/EAP' or 'MAC Address', Encryption method is WPA, WPA2, WPA mixed, or none. 2) Authentication method is 'Open', Encryption method is WPA, WPA2 (Algorithm may not be Auto), enable Zero-IT Activation, enable Dynamic PSK.

Example

```
ruckus(config-wlan)# dynamic-vlan
```

The command was executed successfully. To save the changes, type 'end' or 'exit'

no dynamic-vlan

To disable dynamic VLAN, use the following command:

```
no dynamic-vlan
```

Syntax Description

no dynamic-vlan	Disable dynamic VLAN
-----------------	----------------------

Defaults

Disabled.

Example

```
ruckus(config-wlan)# no dynamic-vlan
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

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
```

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
```

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
```

roaming-acct-interim-update

To enable accounting interim-updates when a client roams, use the following command:

```
roaming-acct-interim-update
```

When “roaming-acct-interim-update” is set, all traffic and session-id data from the original session is carried over to the new session.

Defaults

Disabled.

no roaming-acct-interim-update

To disable accounting interim updates when a client roams (default: disabled), use the following command:

```
no roaming-acct-interim-update
```

zero-it-activation

To enable Zero-IT activation, use the following command:

```
zero-it-activation  
zero-it
```

Syntax Description

zero-it-activation	Enable Zero-IT activation
zero-it	Enable Zero-IT activation

Defaults

Disabled.

Example

```
ruckus(config-wlan)# zero-it-activation
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

no zero-it-activation

To disable Zero-IT activation, use the following command:

```
no zero-it-activation  
no zero-it
```


Syntax Description

no zero-it-activation	Disable Zero-IT activation
no zero-it	Disable Zero-IT activation

Defaults

Disabled.

Example

```
ruckus(config-wlan)# no zero-it
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

no l2acl

To disable Layer 2 Access Control Lists, use the following command:

```
no l2acl
```

no role-based-access-ctrl

To disable role based access control policy service, use the following command:

```
no role-based-access-ctrl
```

no l3acl

To disable Layer 3/4 ACLs, use the following command:

```
no l3acl
```

no vlanpool

To disable the VLAN pool for this WLAN, use the following command:

```
no vlanpool
```

no dvcpcy

To disable device policy for this WLAN, use the following command:

```
no dvcpcy
```

rate-limit

To set the rate limiting for the WLAN, use the following command:

```
rate-limit uplink <NUMBER> downlink <NUMBER>
```

Syntax Description

rate-limit	Set the rate limit
uplink	Set the uplink rate limit
downlink	Set the downlink rate limit
<NUMBER>	Set the rate limiting to the value specified.

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'.

vlanpool

To configure a VLAN pool with the specified name, use the following command:

```
vlanpool <WORD>
```

no mac-addr-format

Sets MAC auth username and password to format aabbccddeeff.

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:f f	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.

<code>mac-addr-format</code> <code>AA:BB:CC:DD:EE:F</code> <code>F</code>	Sets MAC auth username and password to format AA:BB:CC:DD:EE:FF.
---	---

acl dvcpcy

To apply a Device Policy to the WLAN, use the following command:

```
acl dvcpcy <WORD>
```

show

To display the WLAN settings, use the following command:

```
show
```

Syntax Description

<code>show</code>	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
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
White List = No ACLS
Application Visibility = disabled
Apply Policy Group = No_Denys
Wlan Bind = all

ruckus(config)#
```

Configure WLAN Group Settings Commands

Use the `wlan-group` commands to configure the settings of a particular WLAN group.

wlan-group

To update the default WLAN group “Default”, use the following command:

```
wlan-group <Default>
```

Syntax Description

<code>wlan-group</code>	Update the WLAN group
<code><WORD></code>	Name of the WLAN group, now only default “Default”

Defaults

Default.

Example

```
ruckus# config
ruckus(config)# wlan-group Default
The WLAN group entry 'Default' has been loaded. To save the WLAN
group, type 'end' or 'exit'.
ruckus(config-wlangrp)#
```

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

<code>abort</code>	Exit the WLAN group without saving changes
--------------------	--

Defaults

None.

Example

```
ruckus# config
ruckus(config)# wlan-group Default
The WLAN group entry 'Default' has been loaded. 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

<code>end</code>	Save changes, and then exit the WLAN group
------------------	--

Defaults

None.

Example

```
ruckus# config
ruckus(config)# wlan-group Default
The WLAN group entry 'Default' has been loaded. 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

<code>exit</code>	Save changes, and then exit the WLAN group
-------------------	--

Defaults

None.

Example

```
ruckus# config
ruckus(config)# wlan-group Default

The WLAN group entry 'Default' 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

<code>quit</code>	Exit the WLAN group without saving changes
-------------------	--

Defaults

None.

Example

```
ruckus# config
ruckus(config)# wlan-group Default
The WLAN group entry ' Default' has been loaded. To save the WLAN
group, type 'end' or 'exit'.
ruckus(config-wlangrp)# quit
No changes have been saved.
ruckus(config)#
```

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

<code>wlan</code>	Add a WLAN to the WLAN group
<code><WORD></code>	Name of the WLAN to be added

Defaults

None.

Example

```
ruckus(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= Default

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
wlan 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
wlan 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 Master. To run these commands, you must first enter the `config-role` context.

role

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

```
role <WORD>
```

Syntax Description

role	Create or modify a user role
<WORD>	Name of role

Defaults

None.

Example

```
ruckus(config)# role role1
The role entry 'role1' has been created
ruckus(config-role)#
```

no role

To delete a role entry from the list, use the following command:

```
no role <WORD>
```

Syntax Description

no role	Delete a user role
<WORD>	Name of role

Defaults

None.

Example

```
ruckus(config)# no role role1
The Role 'role1' has been deleted.
ruckus(config)#
```

abort

To exit the `config-role` context without saving changes, use the `abort` command. Enter this command from within the context of the role that you are configuring.

abort

Syntax Description

abort	Exit the role without saving changes
-------	--------------------------------------

Defaults

None.

Example

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

end

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

```
end
```

Syntax Description

end	Save changes, and then exit the context
-----	---

Defaults

None.

Example

```
ruckus(config-role)# end  
The Role entry has saved successfully.  
Your changes have been saved.  
ruckus(config)#
```

exit

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

```
exit
```

Syntax Description

exit	Save changes, and then exit the context
------	---

Defaults

None.

Example

```
ruckus(config-role)# exit  
The Role entry has saved successfully.  
Your changes have been saved.  
ruckus(config)#
```

quit

To exit the `config-role` context without saving changes, use the `quit` command. Enter this command from within the context of the role that you are configuring.

```
quit
```

Syntax Description

quit	Exit the role without saving changes
------	--------------------------------------

Defaults

None.

Example

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

name

To set the name of a user role, use the following command:

```
name <WORD>
```

Syntax Description

name	Set the name of a user role
<WORD>	Set to this role

Defaults

None.

Example

```
ruckus(config-role)# name guest33
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

description

To set the description for a user role, use the following command:

```
description <WORD>
```

Syntax Description

description	Set the description of a user role
<WORD>	Set to this description

Defaults

None.

Example

```
ruckus(config-role)# description testforCLI
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

group-attributes

To set the group attributes of a user role, use the following command:


```
group-attributes <WORD>
```

Syntax Description

group-attributes	Set the attributes of a user role
<WORD>	Set to this attribute

Defaults

None.

Example

```
ruckus(config-role)# group-attributes ruckus1
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

wlan-allowed

To set the WLANs to which a user role will have access, use the following command:

```
wlan-allowed [all | specify-wlan]
```

Syntax Description

wlan-allowed	Set the WLANs to which a role will have access
all	Grant access to all WLANs
specify-wlan	Grant access to a specific WLAN

Defaults

None.

Example

```
ruckus(config-role)# wlan-allowed all
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

```
ruckus(config-role)# wlan-allowed specify-wlan
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

no specify-wlan-access

To remove a particular WLAN from the list of WLANs that a user role can access, use the following command:

```
no specify-wlan-access <WORD/SSID>
```

Syntax Description

no specify-wlan-access	Remove access to a WLAN by a user role
<WORD/SSID>	Remove access to this WLAN

Defaults

None.

Example

```
ruckus(config-role)# no specify-wlan-access joejoe98
```

The wlan 'joejoe98' has been removed from the Role.

specify-wlan-access

To add a particular WLAN to the list of WLANs that a user role can access, use the following command:

```
specify-wlan-access <wlan_ssid>
```

Syntax Description

specify-wlan-access	Add access to a WLAN by a user role
<wlan_ssid>	Add access to this WLAN

Defaults

None.

Example

```
ruckus(config-role)# specify-wlan-access joejoe98
```

The wlan 'joejoe98' has been added to the Role.

no guest-pass-generation

To remove guest pass generation privileges from a user role, use the following command:

```
no guest-pass-generation
```

Syntax Description

no guest-pass-generation	Remove guest pass generation privileges from a user role
--------------------------	--

Defaults

None.

Example

```
ruckus(config-role)# no guest-pass-generation
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

guest-pass-generation

To add guest pass generation privileges to a user role, use the following command:

```
guest-pass-generation
```

Syntax Description

guest-pass-generation	Add guest pass generation privileges to a user role
-----------------------	---

Defaults

None.

Example

```
ruckus(config-role)# guest-pass-generation
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

no admin

To remove Unleashed administration privileges from a user role, use the following command:

```
no admin
```

Syntax Description

no admin	Remove Unleashed administration privileges from a user role
----------	---

Defaults

None.

Example

```
ruckus(config-role)# no admin
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

admin

To add Unleashed administration privileges to a user role, use the following command:

```
admin [super | operator | monitoring]
```

Syntax Description

admin	Add Unleashed 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'.

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

Unleashed 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
```

os-type-allowed all

Allows all OS types to access.

```
os-type-allowed all
```

os-type-allowed specify

Specifies OS types access.

```
os-type-allowed specify
```

specify-os-type-access

Adds the specify OS type into the role entry.

```
specify-os-type-access <WORD>
```

Defaults

None

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)# os-type-allowed specify
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

```
ruckus(config-role)# specify-os-type-access Windows
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

```
ruckus(config-role)#
```

no specify-os-type-access

Deletes the specify OS type from the role entry.

```
no specify-os-type-access <WORD>
```

vlan

Sets the VLAN ID to the specified ID number or "none"

```
vlan <NUMBER>
```

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
```

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 Unleashed  
    Administration:  
      Status= Disallowed  
    Allow All WLANs:  
      Mode= Allow Specify WLAN access
```


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

<code>user</code>	Create or modify a user entry
<code><WORD></code>	Name of the user

Defaults

None.

Example

```
ruckus(config)# user johndoe  
The User entry 'johndoe' has been created.  
ruckus(config-user)#
```

no user

To delete a user record, use the following command:

```
no user <WORD>
```

Syntax Description

<code>user</code>	Create or modify a user entry
<code><WORD></code>	Name of the user

Defaults

None.

Example

```
ruckus(config)# no user johndoe  
The User 'johndoe' has been deleted.  
ruckus(config)#
```

abort

To exit the `config-user` context without saving changes, use the `abort` command. Enter this command from within the context of the user that you are configuring.

```
abort
```

Syntax Description

abort	Exit the user settings without saving changes
-------	---

Defaults

None.

Example

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

end

To save changes, and then exit the `config-user` context, use the following command (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

<code>quit</code>	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

<code>user-name</code>	Set the name of a user
<code><WORD></code>	Set to this user name

Defaults

None.

Example

```
ruckus(config-user)# user-name joel
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

full-name

To set the full name of a user, use the following command:

```
full-name <WORD>
```

Syntax Description

full-name	Set the full name of a user
<WORD>	Set to this full name

Defaults

None.

Example

```
ruckus(config-user)# full-name joejoe
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

password

To set the password of a user, use the following command:

```
password <WORD>
```

Syntax Description

password	Set the password of a user
<WORD>	Set to this password

Defaults

None.

Example

```
ruckus(config-user) # password 1234
```

To assign a role to a user, use the following command:

```
role <WORD>
```

Syntax Description

role	Assign a role to a user
<WORD>	Assign this role

Defaults

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= joe1  
Full Name= joejoe  
Password= 1234  
Role= guest
```

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
```

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 [min|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>
```

Options

1-Device Screen

2-Mobile

3-Email

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

To enable guest pass authentication for this guest access service, use the following command:

```
authentication guest-pass
```

Syntax Description

authentication guest-pass	Enable guest pass authentication
---------------------------	----------------------------------

Example

```
ruckus(config-guest-access)# authentication guest-pass
```

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.

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.

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)#
```

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 = guestservice1
  Onboarding Portal:
    Aspect = Guest pass and ZeroIT
  Authentication:
    Mode = Use guest pass authentication
    Multiple users to share a single guest pass = Disallowed
  Title = Welcome to the Guest Access login page.
  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(config-guest-access)#
```

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>
```

<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 Master'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

```
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

```
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

```
ruckus(config-hotspot)# grace-period 20
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

auth-server local

To use Unleashed 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 Unleashed 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 802.1Xformatof00-10-A4-23-19-C0(bydefault 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 whitelist.

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)#
```

whitelist

To apply a client isolation whitelist to this Hotspot, use the following command:

```
whitelist name <WORD>
```

location-id

To set the location ID of the hotspot, use the following command:

```
location-id <location-id>
```

Syntax Description

<code>location-id</code>	Set the location ID of the hotspot
<code><location-id></code>	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

<code>location-name</code>	Set the location name of the hotspot
<code><location-name></code>	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

<code>restrict-access-order</code>	Add a restrict access order
<code><NUMBER></code>	Add this order ID
<code>order <NUMBER></code>	Sets the hotspot rule order.
<code>description <WORD></code>	Sets the hotspot rule description.
<code>type allow</code>	Sets the hotspot rule type to 'allow'.
<code>type deny</code>	Sets the hotspot rule type to 'deny'.
<code>destination address <IP-ADDR/ WORD></code>	Sets the destination address of a hotspot rule.
<code>destination port <NUMBER/ WORD></code>	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.

The same commands are available for IPv6 networks from the `config-hotspot-restrict-access-ipv6` context.

end

To save changes, and then exit the `config-hotspot-restrict-access` context, use the following command:

```
end
```

Syntax Description

<code>end</code>	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

<code>exit</code>	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 hl_order1
```

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
```

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
```

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 Mesh Commands

Use the `mesh` commands to configure the Master'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

<code>mesh</code>	Configure mesh settings
-------------------	-------------------------

Defaults

none

Example

```
ruckus(config)# mesh  
ruckus(config-mesh)#
```

abort

To exit the `config-mesh` context without saving changes, use the `abort` command.

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:

```
show
```

Syntax Description

show	Display the current mesh settings
------	-----------------------------------

Defaults

None.

Example

```
ruckus(config-mesh)# show
Mesh Settings:
Mesh Status= Enabled
Mesh Name(ESSID)= Mesh-00000000311
Mesh Passphrase= GdxW5CUgNn_SEHOPyCSxv_chHSca MH-OpnRGfX sRvwXBJL-
wUsD64eK8CMEZfm
Mesh Hop Detection:
Status= Disabled
Mesh Downlinks Detection:
Status= Disabled
Tx. Rate of Management Frame=2Mbps
Beacon Interval= 200ms
ruckus(config-mesh)#
```

ssid

To set the SSID of the mesh network, use the following command:

```
ssid <WORD/SSID>
```

Syntax Description

ssid	Set the SSID of the mesh network
------	----------------------------------

<WORD/SSID>

Set to this SSID

Defaults

None.

Example

```
ruckus(config-mesh)# ssid rks_mesh
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

passphrase

To set the passphrase that allows access to the mesh network, use the following command:

```
passphrase <WORD>
```

Syntax Description

passphrase	Set the passphrase that allows access to the mesh network
------------	---

<WORD>	Set to this passphrase
--------	------------------------

Defaults

None.

Example

```
ruckus(config-mesh)# passphrase test123456
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

hops-warn-threshold

To enable and configure the mesh hop threshold, use the following command:

```
hops-warn-threshold <NUMBER>
```

Syntax Description

hops-warn-threshold	Set the mesh hop threshold (max hops)
<NUMBER>	Set to this threshold value

Defaults

5

Example

```
ruckus(config-mesh)# hops-warn-threshold 6
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

no detect-hops

To disable the mesh hop threshold, use the following command:

```
no detect-hops
```

Syntax Description

no detect-hops	Disable the mesh hop threshold
----------------	--------------------------------

Defaults

None.

Example

```
ruckus(config-mesh)# no detect-hops
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

fan-out-threshold

To enable and configure the mesh downlink threshold, use the following command:

```
fan-out-threshold <NUMBER>
```

Syntax Description

fan-out-threshold	Set the mesh downlink threshold (max downlinks)
<NUMBER>	Set to this threshold value

Defaults

5

Example

```
ruckus(config-mesh)# fan-out-threshold 8
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

no detect-fanout

To disable the mesh downlink threshold, use the following command:

```
no detect-fanout
```

Syntax Description

no detect-fanout	Disable the mesh downlink threshold
------------------	-------------------------------------

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) #
```

Configure Alarm Commands

Use the `alarm` commands to configure the Master's alarm notification settings. To run these commands, you must first enter the `config-alarm` context.

alarm

To enter the `config-alarm` context, use the following command.

```
alarm
```

Example

```
ruckus(config) # alarm  
ruckus(config-alarm) #
```

no alarm

To disable alarm settings, use the following command:

```
no alarm
```

Example

```
ruckus(config) # no alarm  
The Alarm settings have been updated.  
ruckus(config) #
```

abort

To exit the `config-alarm` context without saving changes, use the `abort` command.

```
abort
```

Syntax Description

<code>abort</code>	Exit the alarm settings without saving changes
--------------------	--

Defaults

None.

Example

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

end

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

```
end
```

Syntax Description

<code>end</code>	Save changes, and then exit the context
------------------	---

Defaults

None.

Example

```
ruckus(config-alarm)# end  
The Alarm settings have been updated.  
Your changes have been saved.  
ruckus(config)#
```

exit

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

```
exit
```

Syntax Description

<code>exit</code>	Save changes, and then exit the context
-------------------	---

Defaults

None.

Example

```
ruckus(config-alarm)# exit  
The Alarm settings have been updated.  
Your changes have been saved.
```

quit

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

```
quit
```

Syntax Description

<code>quit</code>	Exit the alarm settings without saving changes
-------------------	--

Defaults

None.

Example

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

show

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

```
show
```

Syntax Description

<code>show</code>	Display the current alarm settings
-------------------	------------------------------------

Defaults

None.

Example

```
ruckus(config)# alarm
ruckus(config-alarm)# show
Alarm:
  Status= Enabled
  Email Address= johndoe@gmail.com
  E-mail From = Unleashed@ruckuswireless.com
  SMTP Server Name= smtp.gmail.com
  SMTP Server Port= 587
  SMTP Authentication Username= johndoe@gmail.com
  SMTP Authentication Password= *****
  wait time=
  SMTP Encryption Options:
    TLS= Enabled
    STARTTLS= Enabled

ruckus(config-alarm)#
```

Configure Alarm-Event Settings

Use the alarm-event commands to configure which events will trigger Unleashed 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

ap-lost-contacted	AP lost contact
ssid-spoofing-ap-detected	SSID spoofing AP detected
mac-spoofing-ap-detected	MAC spoofing AP detected
rogue-dhcp-server-detected	Rogue DHCP server expired
lan-rogue-ap-detected	LAN Rogue AP detected
radius-server-unavailable	radius authentication server unreachable
ap-has-hardware-problem	AP hardware problem radius-
radius-accounting-server-unavailable	radius accounting server unreachable
gateway-unreachable	gateway unreachable
ap-radio-on	ap radio on
ap-radio-off	ap radio off
master-switch	master switch
ap-join-with-reason	ap join with reason

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_AP_lost= enabled
MSG_SSID_spoofing_AP_detected = enabled
MSG_MAC_spoofing_AP_detected= enabled
MSG_admin_rogue_dhcp_server = enabled
MSG_same_network_spoofing_AP_detected = enabled
MSG_RADIUS_auth_unavailable = enabled
MSG_AP_hardware_problem = enabled
MSG_RADIUS_acct_unavailable = enabled
MSG_GATEWAY_unreachable = enabled
MSG_AP_RADIO_ON = enabled
MSG_AP_RADIO_OFF = enabled
UN_switch_role = enabled
MSG_AP_joined_with_reason = 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

Example

```
ruckus(config-alarm-event) # no event aaa-server-unreachable
ruckus(config-alarm-event) # show
Alarm Events Notify By Email:
  MSG_AP_lost= disabled
  MSG_SSID_spoofing_AP_detected = disabled
  MSG_MAC_spoofing_AP_detected= disabled
  MSG_admin_rogue_dhcp_server = disabled
  MSG_same_network_spoofing_AP_detected= disabled
  MSG_RADIUS_auth_unavailable = disabled
  MSG_AP_hardware_problem= disabled
  MSG_RADIUS_acct_unavailable = disabled
  MSG_GATEWAY_unreachable= disabled
  MSG_AP_RADIO_ON = disabled
  MSG_AP_RADIO_OFF= disabled
  UN_switch_role = disabled
  MSG_AP_joined_with_reason= disabled

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-adjust-ap-power

To enable the auto adjustment of the AP radio power, which helps optimize radio coverage when radio interference is present, use the following command:

```
auto-adjust-ap-power
```

Syntax Description

auto-adjust-ap-power	Enable the auto adjustment of the AP radio power
----------------------	--

Defaults

Disabled.

Example

```
ruckus(config-services)# auto-adjust-ap-power
The command was executed successfully.
```

no auto-adjust-ap-power

To disable the auto adjustment of the AP radio power, which helps optimize radio

coverage when radio interference is present, use the following command:

```
no auto-adjust-ap-power
```

Syntax Description

no auto-adjust-ap-power	Disable the auto adjustment of the AP radio power
-------------------------	---

Defaults

Disabled.

Example

```
ruckus(config-services)# no auto-adjust-ap-power  
The command was executed successfully.
```

auto-adjust-ap-channel

To enable the auto adjustment of the AP radio channel when radio interference is present, use the following command:

```
auto-adjust-ap-channel
```

Syntax Description

auto-adjust-ap-channel	Enable the auto adjustment of the AP radio channel
------------------------	--

Defaults

None.

Example

```
ruckus(config-services)# auto-adjust-ap-channel  
The command was executed successfully.
```

no auto-adjust-ap-channel

To disable the auto adjustment of the AP radio channel when radio interference is present, use the following command:

```
no auto-adjust-ap-channel
```

Syntax Description

no auto-adjust-ap-channel	Disable the auto adjustment of theAP radio channel
---------------------------	--

Defaults

None.

Example

```
ruckus(config-services)# no auto-adjust-ap-channel
```

The command was executed successfully.

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

Defaults

Enabled for both 2.4 and 5 GHz radios

MTBC: 100

Example

```
ruckus(config-services)# channelfly radio-2.4 100  
The command was executed successfully.  
ruckus(config-services)#
```

Example

```
ruckus(config-services)# channelfly radio-2.4-mtbc 100  
The command was executed successfully.  
ruckus(config-services)#
```

no channelfly

To disable ChannelFly channel management, use the following command:

```
no channelfly [radio-2.4 | radio-5]
```

Syntax Description

no channelfly	Disable ChannelFly automatic adjustment of theAP radio channel
radio-2.4	Disable ChannelFly on the 2.4 GHz radio
radio-5	Disable ChannelFly on the 5 GHz radio

Defaults

None.

Example

```
ruckus(config-services)# no channelfly radio-2.4  
The command was executed successfully.  
ruckus(config-services)# no channelfly radio-5  
The command was executed successfully.  
ruckus(config-services)#
```


background-scan

To enable background scanning and configure the scan interval, use the following command:

```
background-scan [radio-2.4-interval | radio-5-interval]
<NUMBER>
```

Syntax Description

background-scan	Enable background scanning and configure the scan interval
radio-2.4-interval	Configure background scanning interval for the 2.4 GHz radio
radio-5-interval	Configure background scanning interval for the 5GHz radio
<NUMBER>	Perform background scan at this interval (in seconds)

Defaults

20 seconds

Example

```
ruckus(config-services)# background-scan radio-2.4-interval 6
The command was executed successfully.
```

no background-scan

To disable background scanning on the 2.4GHz radio, use the following command:

```
no background-scan [radio-2.4|radio-5]
```

Syntax Description

no background-scan	Disable background scanning
radio-2.4	Disable background scanning on the 2.4GHz radio
radio-5	Disable background scanning on the 5GHz radio

Defaults

None

Example

```
ruckus(config-services)# no background-scan radio-2.4
```

The command was executed successfully.

```
ruckus(config-services)# no background-scan radio-5
```

The command was executed successfully.

aeroscout-detection

To enable detection of AeroScout RFID Tags by APs that are managed by ZoneDirertor, use the following command:

```
aeroscout-detection
```

Syntax Description

aeroscout-detection	Enable detection of AeroScout RFID Tags by APs
---------------------	--

Defaults

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)#
```

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

<code>help</code>	Shows available commands
<code>history</code>	Shows a list of previously run commands
<code>end</code>	Saves changes, and the exits the <code>config-wips</code> context
<code>exit</code>	Saves changes, and the exits the <code>config-wips</code> context
<code>no <WORD></code>	Disable WIPS services
<code>protect-excessive-wireless-request</code>	<ssid-spoofing same-network user-blocked mac-spoofing>
<code>temp-block-auth-failed-client time <NUMBER></code>	
<code>rogue-report <[all] [malicious</code>	

Enables protecting the wireless network against excessive wireless requests

Temporarily block wireless clients with repeated authentication failures for the specified time (in seconds)

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 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>
```

Configuring a 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 mdnssproxyrule	Delete mDNSproxy rule
mdnssproxyrule <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>
```

Configuring mDNS Proxy Rules

The following commands can be used from within the `config-mdnssproxyrule` 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)#
```

Using Debug Commands

4

In this chapter:

- [Debug Commands Overview](#)
- [General Debug Commands](#)
- [Show Commands](#)
- [Accessing a Remote AP CLI](#)
- [Working with Debug Logs and Log Settings](#)
- [Remote Troubleshooting](#)
- [AP Core Dump Collection](#)
- [Script Execution](#)

Debug Commands Overview

This section describes the commands that you can use to debug ZoneDirector and connected APs, and to configure debug log settings. From the privileged commands context, type **debug** to enter the debug context. To show a list of commands available from within the debug context, type help or ?.

General Debug Commands

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

help

Shows available commands.

list-all

List all available commands.

history

Shows a list of previously run commands.

quit

Exits the debug context.

delete-station

To deauthorize the station with the specified MAC address, use the following command.

```
delete-station <MAC>
```

Syntax Description

<code>delete-station</code>	Delete the station with the specified MAC address
<code><MAC></code>	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

<code>restart-ap</code>	Restart the device with the specified MAC address
<code><MAC></code>	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

<code>wlaninfo</code>	Enable logging of WLAN info
<code><OPTIONS></code>	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: disabledTimeout:10

```

*** Total WLAN Entries: 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)#
```

save-config

Upload the configuration file to the designated TFTP site.

```
save-config <IP-ADDR> <FILE-NAME>
```

Syntax Description

save-config	Upload the configuration file
<IP-ADDR>	The destination IP address
<FILE-NAME>	The destination file name

Defaults

None.

Example

```
ruckus(debug)# save-config 192.168.11.26 config.log  
Creating backup config file  
Done  
Uploading backup config file  
...  
ruckus(debug)#
```

Show Commands

This section describes the show commands available within the debug context.

show ap

Displays a list of all approved devices.

```
show ap
```

Syntax Description

show ap	Display a list of all approved APs
---------	------------------------------------

Defaults

None.

Example

```
ruckus(debug) # show ap
AP:
  ID:
    1:
      MAC Address= 6c:aa:b3:3d:66:30
      Model= r500
      Approved= Yes
      Device Name= R500-Unleashed
      ...
      ...
ruckus(debug) #
```

show station

Displays a list of all connected stations (or clients).

```
show station
```

Syntax Description

show station	Show all connected stations
--------------	-----------------------------

Defaults

None.

Example

```
ruckus(debug) # show station
Clients List:
Client:
  MAC Address= 6c:62:6d:1b:e3:00
  User Name=
  IP Address= 192.168.11.11
  IPv6 Address=
  Access Point= 04:4f:aa:0c:b1:00
  WLAN= Ruckus1
  Channel= 1
  Signal (dB)= 53

Client:

  MAC Address= 00:22:fb:ad:1b:2e
  User Name=
  IP Address= 192.168.11.7
  IPv6 Address=
  Access Point= 04:4f:aa:0c:b1:00
  WLAN= Ruckus1
  Channel= 165
  Signal (dB)= 42

ruckus(debug) #
```

show logs

Displays a list of debug log components.

```
show logs
```

Syntax Description

show logs	Display debug log components
-----------	------------------------------

Defaults

None.

Example

```
ruckus(debug)# show logs
Debug Logs:
  All= Enabled
  Sys-mgmt= Enabled
  Mesh= Enabled
  Web-auth= Enabled
  Rf-mgmt= Enabled
  Radius= Enabled
  Hotspot-srv= Enabled
  Aps= Enabled
  Net-mgmt= Enabled
  802.1x= Enabled
  Web-svr= Enabled
  802.11= Enabled
  Dvlan= Enabled
    = Enabled
  Debug logs of specified MAC address:
    Status= Disabled
ruckus(debug)#
```

show remote-troubleshooting

Shows remote-troubleshooting status.

```
show remote-troubleshooting
```

Syntax Description

show remote-	
troubleshooting	Display remote troubleshooting status

Defaults

None.

Example

```
ruckus(debug)# show remote-troubleshooting
```

Ruckus CA troubleshooting is stopped!

The server addr is: None

```
ruckus(debug)#
```

ps

Displays information about all processes that are running (ps -aux).

```
ps
```

Syntax Description

ps	Display a list of all running processes
----	---

Defaults

None.

Example

```
ruckus (debug) # ps
```

PID	PPID	USER	VSZ	STAT	COMMAND
1	0	ruckus	1200	S	init
2	1	ruckus	0	SWN	[ksoftirqd/0]
3	1	ruckus	0	SW	[watchdog/0]
4	1	ruckus	0	SW<	[events/0]
5	1	ruckus	0	SW<	[khelper]
6	1	ruckus	0	SW<	[kthread]
7	6	ruckus	0	SW<	[kblockd/0]
8	6	ruckus	0	SW<	[khubd]
9	6	ruckus	0	SW	[pdflush]
10	6	ruckus	0	SW	[pdflush]
12	6	ruckus	0	SW<	[aio/0]
11	1	ruckus	0	SW	[kswapd0]
13	1	ruckus	0	SW	[mtdblockd]
14	6	ruckus	0	SW<	[scsi_ah_0]
15	6	ruckus	0	SW<	[usb-storage]
17	6	ruckus	0	SW<	[V54_bodygard/0]

```

18      1 ruckus      0 SW    [pktgen/0]
29      6 ruckus      0 SW<   [reiserfs/0]
104     1 ruckus      956 S   /usr/sbin/in.tftpd -l -s /etc/
airespider-images
110     1 ruckus      660 S   /bin/wd_feeder
242     1 ruckus     2572 S   /bin/emf_repo_flashsync monitor 15
243     1 ruckus      944 S   ttylogd
246     1 ruckus      0 SW<   [uif-246]
260     1 ruckus     14492 S   stamgr -d3 -t0
266     260 ruckus     14492 S   stamgr -d3 -t0
267     266 ruckus     14492 S <   stamgr -d3 -t0
268     266 ruckus     14492 S   stamgr -d3 -t0
269     1 ruckus     2268 S   apmgr
277     269 ruckus     2268 S   apmgr
278     277 ruckus     2268 S <   apmgr
299     1 ruckus     19564 S   emfd
316     299 ruckus     19564 S   emfd
317     316 ruckus     19564 S   emfd
318     316 ruckus     19564 S   emfd
322     1 ruckus     1108 S   /usr/sbin/dropbear -e /bin/login.sh
-r /etc/air
328     1 ruckus     1188 S   /bin/sh /bin/login.sh
329     1 ruckus     1188 S   /bin/sh /bin/tacmon.sh
331     1 ruckus      676 S   /bin/rhttpd
332     1 ruckus     1140 S <   /bin/zapd
333     1 ruckus     1100 S <   /bin/clusterD
334     328 ruckus      856 S   /bin/login
335     329 ruckus      680 S   /bin/tacmon -i 30 -r 15
347     1 ruckus      808 S   /bin/tsyslogd -r -h -n --rotate=7
368     277 ruckus     2268 S <   apmgr
369     277 ruckus     2268 S <   apmgr
572     1 ruckus     1184 S   /sbin/udhcpd -i br0 --
pidfile=/var/ run/udhcpd.p
580     316 ruckus     19564 S   emfd
612     316 ruckus     19564 S   emfd
616     316 ruckus     19564 S   emfd
622     316 ruckus     19564 S   emfd
624     299 ruckus     6132 S <   webs &
625     316 ruckus     19564 S   emfd
637     624 ruckus     6132 S   webs &
638     637 ruckus     6132 S <   webs &
639     637 ruckus     6132 S <   webs &

```

```

640    637 ruckus    6132 S <  webs &
641    637 ruckus    6132 S <  webs &
642    637 ruckus    6132 S    webs &
655    637 ruckus    6132 S <  webs &
656    637 ruckus    6132 S <  webs &
20503  316 ruckus    19564 S    emfd
30679   1 ruckus     2672 S    /usr/sbin/vsftpd /etc/vsftpd2.conf
10220  322 ruckus    1184 S    /usr/sbin/dropbear -e /bin/login.sh
-r /etc/air
10221 10220 ruckus     1188 S    /bin/sh /bin/login.sh
10222 10221 ruckus      856 S    /bin/login
10223 10222 ruckus     7972 S    ruckus_cli2
10426 10223 ruckus     1188 S    sh -c /bin/ps -aux
10427 10426 ruckus     1188 R    /bin/ps -aux
ruckus (debug) #

```

Accessing a Remote AP CLI

The following command is used to access the command line interface of a connected AP and execute AP CLI commands from Unleashed. Configuration changes made through the AP CLI may be overwritten by Unleashed settings if the AP is restarted or reconnects to Unleashed.

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

<code>remote_ap_cli</code>	Execute CLI commands in a remote AP
<code>-q</code>	Do not display results
<code>-a</code>	Specify AP by MAC address
<code>ap_mac</code>	The AP's MAC address
<code>-A</code>	All connected APs
<code>cmd</code>	AP CLI command
<code>arg</code>	AP CLI command argument

Example

```
ruckus(debug)# remote_ap_cli -A "get version"
---- Command 'rkscli -c "get version"' executed at
6c:aa:b3:3d:66:30
Ruckus R500 Multimedia Hotzone Wireless AP
Version: 200.3.9.13.14883570
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 Unleashed debug logs.

logs all

Enables debug logs of all debug components.

NOTE Running this command can place considerable load on the system. If your Unleashed 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.

Syntax Description

logs all	Enable logging of all debug components
----------	--

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
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  
  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 bonjour-gateway

Enable Bonjour Gateway debug logs.

no logs comp bonjour-gateway

Disable Bonjour Gateway debug logs.

logs comp mDNS

Enable Bonjour mDNS debug logs.

no logs comp mDNS

Disable Bonjour mDNS 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

<code>logs</code>	Enable debug logs
<code>mac</code>	Filter logs by specific MAC address
<code><MAC></code>	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 play

Starts displaying logs on console.

CAUTION! Running this command can place considerable load on the system. If your Unleashed 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.

Syntax Description

logs	Enable debug logs
play	Start log play

Example

```
ruckus(debug)# logs play
```

```

ruckus(debug)# [Feb 15 05:53:30][EMFD][debug]jobService-
Func():Executing job[user auth attempt_hash_autoexpire] at
1329285210...
[Feb 15 05:53:30][EMFD][debug]jobServiceFunc():Executing job at
1329285210...Done
[Feb 15 05:53:30][EMFD][debug]jobServiceFunc():Executing
job[station auth attempt_hash_autoexpire] at 1329285210...
[Feb 15 05:53:30][EMFD][debug]jobServiceFunc():Executing job at
1329285210...Done
[Feb 15 05:53:33][STAMgr][debug]acsrvc_thread():ACSRVC rcv AP
04:4f:aa:0c:b1:00, IP= 192.168.11.6, IPv6=fc00::1
...
...
ruckus(debug)# no logs play
ruckus(debug)#

```

no logs 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]jobService-
Func():Executing job[user auth attempt_hash_autoexpire] at
1329285210...
[Feb 15 05:53:30][EMFD][debug]jobServiceFunc():Executing job at
1329285210...Done
[Feb 15 05:53:30][EMFD][debug]jobServiceFunc():Executing
job[station auth attempt_hash_autoexpire] at 1329285210...
[Feb 15 05:53:30][EMFD][debug]jobServiceFunc():Executing job at
1329285210...Done
[Feb 15 05:53:33][STAMgr][debug]acsrvc_thread():ACSRVC rcv AP
04:4f:aa:0c:b1:00, IP= 192.168.11.6, IPv6=fc00::1
...
...
ruckus(debug)# no logs play

```

```
ruckus (debug) #
```

Remote Troubleshooting

This section describes remote troubleshooting commands.

remote-troubleshooting server

To set the remote troubleshooting server IP address, use the following command:

```
remote-troubleshooting server <IP-ADDR>
```

remote-troubleshooting start

Enables remote troubleshooting.

Syntax Description

remote- troubleshooting	Remote troubleshooting
start	Start remote troubleshooting

Defaults

None.

Example

```
ruckus (debug) # remote-troubleshooting start  
ruckus (debug) #
```

remote-troubleshooting stop

Disables remote troubleshooting.

Syntax Description

remote- troubleshooting	Remote troubleshooting
----------------------------	------------------------

`stop` Stop remote troubleshooting

Defaults

None.

Example

```
ruckus(debug) # remote-troubleshooting stop
```

```
ruckus(debug) #
```

AP Core Dump Collection

This section lists the AP core dump commands.

collect_ap_coredump

Enable AP core dump collection.

```
collect_ap_coredump [all|<MAC>]
```

Syntax Description

collect_ap_core dump	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	Stop collecting AP core dump
----	------------------------------

```
collect_ap_core  
dump
```

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

<code>script</code>	Enter the script context
---------------------	--------------------------

Defaults

None.

Example

```
ruckus(debug)# script
ruckus(script)#
```

quit

Exit the script context.

```
quit
```

Syntax Description

<code>quit</code>	Exit the script context
-------------------	-------------------------

Defaults

None.

Example

```
ruckus(script)# quit
ruckus(debug)#
```

list

List all available scripts.

```
list
```

Syntax Description

<code>list</code>	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

<code>info</code>	Display script information
-------------------	----------------------------

Defaults

None.

Example

```
ruckus(script)# info
info <file>
ruckus(script)#
```

exec

Execute script.

```
exec <file> {parameter}
```

Syntax Description

exec	Execute the script
------	--------------------

Defaults

None.

Example

```
ruckus(script)# exec  
exec <file> {parameter}  
ruckus(script)#
```

Example

In this chapter:

- Configure guest-access WLAN
- Run AP CLI

Configure guest-access WLAN

1, configure guest-access server

Create one guest access server for guest-access WLAN.

```
ruckus(config)# guest-access g_ga_b
```

The Guest Access entry 'g_ga_b' has been created. To save the Guest Access entry, type end or exit.

```
ruckus(config-guest-access)#
```

```
ruckus(config-guest-access)#
```

```
ruckus(config-guest-access)# show
```

Guest Access:

Name = g_ga_b

Onboarding Portal:

Aspect = Guest pass and ZeroIT

Authentication:

Mode = Use guest pass authentication

Effective time:

Countdown-by-issued = false

Effective Period = 7 Days

Title = Welcome to the Guest Access login page.

Terms of Use:

Status = Disabled

Redirection:

Mode = To the URL that the user intends to visit

Self Service Registration:

Status = Disabled

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

ruckus(config-guest-access)# end

Your changes have been saved..

2, Configure wlan

Create one wlan, set type to guest-access and guest access server.

```
ruckus(config)# wlan ggk_ga_test
```

The WLAN service 'ggk_ga_test' has been created. To save the WLAN service, type 'end' or 'exit'.

```
ruckus(config-wlan)#
```

```
ruckus(config-wlan)# type guest-access g_ga_b
```

The command was executed successfully. To save the changes, type 'end' or 'exit'.

```
ruckus(config-wlan)#
```

```
ruckus(config-wlan)# show
```

WLAN Service:

ID:

:

NAME = ggk_ga_test

Tx. Rate of Management Frame(2.4GHz) = 2.0Mbps

Tx. Rate of Management Frame(5GHz) = 6.0Mbps

Beacon Interval = 100ms

SSID = ggk_ga_test

Description =

Type = Guest Access

Authentication = open

Encryption = none

FT Roaming = Disabled

802.11k Neighbor report = Disabled

Web Authentication = Enabled

Grace Period:

Status = Enabled

Period = 480 Minutes

Authentication Server = Guest Accounts

Accounting Server = Disabled

Called-Station-Id type = wlan-bssid

Tunnel Mode = Disabled

DHCP relay = Disabled

Background Scanning = Enabled

Max. Clients = 100
Isolation per AP = Enabled
Isolation across AP = Disabled
Zero-IT Activation = Disabled
Priority = High
Load Balancing = Disabled
Band Balancing = Disabled
Rate Limiting Uplink = Disabled
Rate Limiting Downlink = Disabled
Auto-Proxy configuration:
 Status = Disabled
Inactivity Timeout:
 Status = Enabled
 Timeout = 5 Minutes
Web Authentication Timeout = 5 Minutes
VLAN-ID = 1
Dynamic VLAN = Disabled
Closed System = Disabled
Https Redirection = Enabled
OFDM-Only State = Disabled
Multicast Filter State = Disabled
802.11d State = Disabled
Force DHCP State = Disabled
Force DHCP Timeout = 10
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 = Guest
L3/L4/IPv6 Address = Guest
Precedence = Default
Proxy ARP = Disabled
Device Policy = No ACLS
Vlan Pool = No Pools
Role based Access Control Policy = Disabled
SmartRoam = Disabled Roam-factor = 1
White List = No ACLS
Application Visibility = disabled
Apply Policy Group = No_Denys
Wlan Bind = all

```
ruckus(config-wlan)#  
ruckus(config-wlan)# end  
rksmcast currently snooping max of 14 interfaces IGMP(13) MLD(0)  
The WLAN service 'ggk_ga_test' has been updated and saved.  
Your changes have been saved.
```

Run AP CLI

run AP CLI in master AP ap-mode

```
ruckus# ap-mode  
ruckus(ap-mode)# get version  
Ruckus R500 Multimedia Hotzone Wireless AP
```

Version: 200.3.9.13.14891280

OK

```
ruckus(ap-mode)# get election
```

The local AP's ip address is 172.18.151.2, Election role is master, Fix role is NO, Debug level is ERROR

```
mac_address ipaddress role configID station_rate free_memory mesh_enabled  
mesh_node mesh_node_type model version bak_version systime board_type  
last_seen
```

```
-----  
-----  
6c:aa:b3:3d:66:30 172.18.151.1 member 388 44 188296 1 0 1 R500  
200.3.9.13.14891280-----  
200.3.9.13.14889646----- 0 zf7752-3-29-4bss Sun  
Jan 4 01:41:31 1970
```

```
94:f6:65:3c:cf:a0 172.18.151.2 master 388 43 171704 1 0 1 R500  
200.3.9.13.14891280-----  
200.3.9.13.14889646----- 265193 zf7752-3-29-4bss  
Sun Jan 4 01:41:34 1970
```

OK

```
ruckus(ap-mode)#
```

```
ruckus(ap-mode)# set telnet enable
```

OK

```
ruckus(ap-mode)# telnetd ..... [stopped] (0.090)
```

```
telnetd ..... [started] (0.092)
```

```
ruckus(ap-mode)# get telnet
```

Telnet Service is enabled

OK

Run AP CLI in remote_ap_cli
remote_ap_cli

```
ruckus(debug)# remote_ap_cli -A "get version"
---- Command 'rkscli -c "get version"' executed at
6c:aa:b3:3d:66:30
Ruckus R500 Multimedia Hotzone Wireless AP
Version: 200.3.9.13.14883570
OK
---- Command Execution Summary:
      success: 2
      failure: 0
      total: 2
ruckus(debug)#
```



Copyright © 2006-2016. Ruckus Wireless, Inc.
350 West Java Dr. Sunnyvale, CA 94089. USA
www.ruckuswireless.com